НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Побудова віртуальних приватних мереж
на основі обладнання фірми Cisco»

Виконав:
студент IV курсу, групи ТС-61
Волік Дмитро Вадимович _____

Керівник:
Доцент, к.т.н.
Григоренко Олена Григорівна _____

Рецензент:
Посада, науковий ступінь, вчене звання,
Прізвище, ініціали _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студент _____

Київ – 2020 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Програма професійного спрямування (спеціалізація) – «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Леонід УРИВСЬКИЙ

«___»_____20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Воліку Дмитру Вадимовичу

1. Тема роботи «Побудова віртуальних приватних мереж на основі обладнання фірми Cisco», керівник роботи Григоренко Олена Григорівна, доцент, к.т.н., затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом роботи _____

3. Вихідні дані до роботи: віртуальні приватні мережі, протоколи тунелювання, обладнання фірми Cisco

4. Зміст роботи

1) ОСНОВНІ ВІДОМОСТІ ПРО ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ;
2) ПОБУДОВА VPN МЕРЕЖ;
3) СТВОРЕННЯ ЕКСПЕРИМЕНТАЛЬНОГО СТЕНДУ;
4) НАЛАШТУВАННЯ VPN НА ОБЛАДНАННІ ФІРМИ CISCO;
5) ВИСНОВКИ.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Презентація-захист на тему: «Побудова віртуальних приватних мереж

на основі обладнання фірми Cisco»

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання	20.01.2020 – 01.02.2020	
2	Визначення мети дипломної роботи та розробка змісту	01.02.2020 – 10.02.2020	
3	Написання вступної частини дипломної роботи	10.02.2020 – 22.02.2020	
4	Написання першого розділу. Формування основних відомостей про віртуальні приватні мережі	22.02.2020 – 07.03.2020	
5	Написання другого розділу. Пояснення та класифікація технологій тунелювання	07.03.2020 – 22.03.2020	
6	Робота над третім розділом. Розробка та встановлення експериментального стенду	22.03.2020 – 16.04.2020	
7	Написання третього розділу	16.04.2020 – 04.05.2020	
8	Написання четвертого розділу. Налаштування експериментального стенду та перевірка роботи віртуальних приватних мереж на ньому	04.05.2020 – 20.05.2020	
9	Написання загальних висновків	20.05.2020 – 23.05.2020	
10	Оформлення дипломного проекту	23.05.2020 – 30.05.2020	
11	Підготовка презентації до захисту	30.05.2020 – 07.06.2020	

Студент Дмитро ВОЛІК

Керівник роботи Олена ГРИГОРЕНКО

РЕФЕРАТ

Текстова частина дипломної роботи: 76 с., 22 рис., 8 табл., 10 джерел.

Метою роботи є дослідження, аналіз, апаратна реалізація та налаштування віртуальних приватних мереж на обладнанні фірми Cisco.

В даній роботі розглянуто технології створення VPN, основні види тунелювання та протоколи безпеки мережевого трафіку. В практичній частині показано створення експериментального стенду, на якому випробувані дві основні реалізації захищених VPN – Site-to-Site та Remote Access.

ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ, ТУНЕЛЮВАННЯ, БЕЗПЕКА МЕРЕЖЕВОГО ТРАФІКУ, VPN SITE-TO-SITE, ТЕХНОЛОГІЯ ВІДДАЛЕНОГО ДОСТУПУ

ABSTRACT

The purpose of the work is research, analysis, hardware implementation and configuration of virtual private networks based on Cisco equipment.

The work shows VPN creation technologies, basic types of tunneling and network traffic security protocols. The practical part shows the creation of an experimental stand, which tested two main implementations of secure VPNs - Site-to-Site and Remote Access.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ACL	Access Control List	Список Контролю Доступу
AH	Authentication Header	Заголовок Аутентифікації
ASA	Adaptive Security Appliances	Прилади Адаптивної Безпеки
ATM	Asynchronous Transfer Mode	Асинхронна Передача Даних
BGP	Border Gateway Protocol	Протокол Граничного Шлюзу
CE	Client Edge	Граничний Маршрутизатор Клієнта
CEF	Cisco Express Forwarding	Швидке Пересилання від Cisco
CLI	Command Line Interface	Інтерфейс Командного Рядку
DMVPN	Dynamic Multipoint VPN	Динамічна Багаточкова VPN
DRAM	Dynamic Random Access Memory	Динамічна Оперативна пам’ять
GRE	Generic Routing Encapsulation	Загальна Інкапсуляція Маршрутів
IDS	Intrusion Detection System	Система Виявлення Вторгнень
IETF	Internet Engineering Task Force	Відкрите Міжнародне Співтовариство Проектувальників
IGP	Interior Gateway Protocol	Протокол Внутрішніх Шлюзів
IKE	Internet Key Exchange	Інтернет Обмін Ключами
IOS	Internetwork Operating System	Межмережева Операційна Система
IP	Internet Protocol	Інтернет Протокол
IPS	Intrusion Prevention System	Система Запобігання Вторгненням
IPsec	Internet Protocol Security	Захищений Інтернет-протокол
ISAKMP	Internet Security Association and Key Management Protocol	Асоціація Інтернет-Безпеки та Протокол Управління Ключами
L2TP	Layer 2 Tunneling Protocol	Протокол Тунелювання Рівня 2
LAN	Local Area Network	Локальна Комп’ютерна Мережа
MPLS	Multiprotocol Label Switching	Багатопротокольна Комутація за Мітками

NAC	Network Access Control	Мережевий Контроль Доступу
NAT	Network Address Translation	Трансляція Мережевих Адрес
OSI	Open System Interconnection	Модель Взаємодії Відкритих Систем
OSPF	Open Shortest Path First	Динамічний Протокол Маршрутизації Для Знаходження Найкоротшого Шляху
PE	Provider Edge	Граничний Маршрутизатор Провайдера
PPTP	Point-to-Point Tunneling Protocol	Протокол Тунелювання з Точки на Точку
RFC	Request for Comments	Запит Коментарів
SA	Security Association	Об’єднання безпеки
SDM	Security Device Manager	Програма Захищеного Управління Пристроями
SFP	Small Form-Factor Pluggable	Стандарт Модульних Трансиверів
SSL	Secure Sockets Layer	Рівень Захищених Сокетів
TCP	Transmission Control Protocol	Протокол Керування Передачею
TFTP	Trivial File Transfer Protocol	Простий Протокол Передачі Файлів
TLS	Transport Layer Security	Безпека Транспортного Рівня
VC	Virtual Connection	Віртуальне З’єднання
VPN	Virtual Private Network	Віртуальна Приватна Мережа
VRF	Virtual Routing and Forwarding	Віртуальна Маршрутизація та Пересилання
VTI	Vitrual Tunneling Interface	Віртуальний Інтерфейс Тунелювання
WAN	Wide Area Network	Глобальна Мережа
WIC	WAN Interface CARD	Інтерфейсна Карта WAN

ВСТУП

В наш час зростає попит на підключення до внутрішніх мереж з віддалених місць. Працівники часто потребують підключення до внутрішніх приватних мереж через Інтернет (що з самого початку небезпечно) з дому, готелів, аеропортів або з інших зовнішніх мереж. Безпека стає головним фактором, коли співробітники чи ділові партнери мають постійний доступ до внутрішніх мереж із незахищених зовнішніх місць.

Технологія віртуальних приватних мереж - VPN (Virtual Private Network) забезпечує спосіб захисту інформації, що передається через Інтернет, дозволяючи користувачам створити віртуальний приватний «тунель» для безпечного входу у внутрішню мережу, надає доступ до ресурсів, даних та комунікацій через незахищену мережу, таку як Інтернет.

Віртуальні приватні мережі (VPN) використовуються у всьому світі, щоб забезпечити зашифровані підключення до Інтернету [1]. Шифрування приховує діяльність користувачів від сторонніх очей, а також надає можливість користуватися мережею Інтернет з підвищеною конфіденційністю. Більше того, VPN може замінити вашу справжню IP-адресу на іншу з іншого регіону, що дозволяє отримувати інформацію, доступ до якої раніше був заблокований.

Ринок VPN невпинно зростає. Щоб це зрозуміти, досить звернутися до статистики. Згідно з дослідженнями компанії Knowledge Sourcing Intelligence LLP, ринок VPN буде зростати з темпами 6,39% на рік протягом наступних п'яти років [2]. У 2018 році ринок охоплював близько 34,6 мільярда доларів, тож, враховуючи цей темп, до 2024 року його обсяг сягне понад 50 мільярдів доларів. У звіті основна причина зростання попиту – проблеми кібербезпеки. Однак, оскільки VPN направляє дані на інший сервер перед тим, як перенести користувача на потрібну веб-сторінку, з’являються певні проблеми із продуктивністю та швидкістю, що частково стримує попит на ці послуги протягом прогнозованого періоду.

Виходячи з вище наведеного, тема роботи є актуальною.

Метою роботи є дослідження побудови та налаштування віртуальних приватних мереж різних типів.

Об'єктом дослідження є віртуальні приватні мережі

Предмет дослідження - апаратна та програмна реалізація VPN різних типів.

Для досягнення поставленої мети в роботі необхідно вирішити наступні завдання:

1) Надання основних відомостей про віртуальні приватні мережі;

2) Постановка задачі забезпечення безпеки мережевого трафіку та мереж. Надання основних рекомендацій, необхідних політик безпеки та кроки до вирішення даної проблеми;

3) Наведення класифікації віртуальних приватних мереж;

4) Пояснення суті та призначення двох реалізацій VPN – Site-to-Site та Remote Access;

5) Створення експериментального стенду;

6) Описання використаного обладнання, пояснення вибору мережевих пристроїв, їх функціоналу та раціональності використання у даній роботі;

7) За допомогою стенду виконання налаштування основних методів тунелювання, як для Site-to-Site, так і для Remote Access VPN.

1 ОСНОВНІ ВІДОМОСТІ ПРО ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ

1.1 Задача забезпечення безпеки мережевого трафіку та мереж

VPN (Virtual Private Network) - це загальний термін, що використовується для опису комунікаційної мережі, яка використовує будь-яку комбінацію технологій для захисту з'єднання, тунелювання через незахищену або ненадійну мережу.

Для того, щоб віртуальні мережі працювали належним чином та забезпечували вискоий рівень безпеки, необхідно дотримуватися наступних рекомендацій [3]:

- VPN-з'єднання можна посилити за допомогою брандмауерів;
- Для більш ефективного контролю за атаками рекомендується реалізувати системи IDS/IPS (система виявлення/запобігання вторгнень);
- Антивірусне програмне забезпечення має бути встановлено на віддалених клієнтах та мережевих серверах, щоб запобігти поширенню будь-якого вірусу/хробака, якщо інфіковано будь-який з кінців тунелю;
- Небезпечним або некерованим системам з простою аутентифікацією або взагалі без аутентифікації, не можна дозволяти з'єднання VPN до внутрішньої мережі;
- Необхідно забезпечити функції реєстрації та аудиту для запису мережевих з'єднань, особливо будь-яких несанкціонованих спроб доступу. Журнал слід регулярно переглядати;
- Треба проводити навчання адміністраторів мережі /служб безпеки та обслуговуючого персоналу, а також віддалених користувачів, щоб гарантувати, що вони дотримуються кращих практик та політик безпеки під час впровадження та постійного використання VPN;
- Політики безпеки та вказівки щодо відповідного використання VPN та підтримки мережі повинні бути розповсюджені відповідальними сторонами для контролю та управління їх використанням VPN;

- Розміщення точки входу VPN у «демілітаризовану» зону (DMZ) рекомендується для захисту внутрішньої мережі;
- Бажано не використовувати роздільне тунелювання для доступу до Інтернету чи будь-якої іншої незахищеної мережі одночасно під час VPN-з'єднання. Брандмауер та IDS повинні використовуватися для виявлення та запобігання будь-якої потенційної атаки, що надходить з незахищених мереж;
- Доступ до внутрішніх мереж повинен бути обмежений і контрольований.

1.2 Призначення та особливості технології віртуальних приватних мереж (VPN)

Замість використання виділеного з'єднання, такого як орендована лінія, встановлюється "віртуальне" з'єднання між географічно рознесеними користувачами та мережами через спільну або загальнодоступну мережу, наприклад Інтернет. Дані передаються так, ніби вони проходять через приватні з'єднання.

VPN передає дані за допомогою тунелювання. Перед передачею пакету вони інкапсулюються (загортаються) у новий пакет із новим заголовком. Цей заголовок надає інформацію про маршрутизацію, щоб вона могла пройти загальнодоступну мережу, перш ніж досягти своєї кінцевої точки тунелю. Цей логічний шлях, по якому проходять інкапсульовані пакети, називається тунелем. Коли кожен пакет досягає кінцевої точки тунелю, він "деінкапсулюється" і пересилається до кінцевого пункту призначення.

Обидві кінцеві точки тунелю повинні підтримувати один і той же протокол тунелювання. Протоколи тунелювання працюють або на другому рівні моделі OSI (Open System Interconnection) - канальному, або на третьому рівні - мережевому. Найпоширенішими протоколами тунелювання є IPsec, L2TP, PPTP та SSL. Пакет із приватною IP-адресою без маршрутизації може бути надісланий всередині пакету з глобальною унікальною IP-адресою, тим самим поширюючи приватну мережу через Інтернет.

VPN використовує шифрування для забезпечення конфіденційності даних. Після підключення VPN використовує описаний вище механізм тунелювання для інкапсуляції зашифрованих даних у захищений тунель, з відкрито зчитуваними заголовками, які можуть перетинати загальнодоступну мережу. Пакети, передані через загальнодоступну мережу таким чином, не можуть бути «прочитані» без належних ключів розшифровки, тим самим забезпечуючи, щоб дані не розкривались або змінювались яким-небудь чином під час передачі.

VPN також допомагає забезпечити перевірку цілісності даних. Зазвичай це виконується за допомогою дайджесту повідомлень, щоб переконатися, що дані не були підроблені під час передачі.

За замовчуванням VPN не забезпечує та не застосовує сильну аутентифікацію користувача. Користувачі можуть ввести просте ім’я користувача та пароль, щоб отримати доступ до внутрішньої приватної мережі з дому чи через інші незахищені мережі. Тим не менш, VPN підтримує додаткові механізми аутентифікації, такі як смарт-карти, жетони та RADIUS.

VPN надає засоби доступу до захищеної, приватної, внутрішньої мережі через незахищені публічні мережі, такі як Інтернет. Незважаючи на те, що захищений канал зв’язку можна відкривати та тунелювати через незахищену мережу через VPN, безпеку на стороні клієнта також варто брати до уваги.

1.3 Класифікація віртуальних приватних мереж

Віртуальні приватні мережі можна класифікувати наступним чином [3]:

- VPN на основі брандмауера - це ті, які оснащені як брандмауером, так і можливостями VPN. Цей тип VPN використовує механізми захисту в брандмауерах для обмеження доступу до внутрішньої мережі. Особливості, які вона надає, включають в себе трансляцію IP-адрес (технологія NAT – Network Address Translation), аутентифікацію користувачів, сповіщення про загрози в режимі реального часу та журнал загроз.

- VPN на основі апаратних засобів забезпечує високу пропускну здатність мережі, кращу продуктивність та більшу надійність, оскільки немає витрат на процесор. Однак це і дорожче.
- VPN на основі програмного забезпечення забезпечує найбільшу гнучкість в управлінні трафіком. Цей тип підходить, коли кінцеві точки VPN не контролюються однією стороною та де використовуються різні брандмауери та маршрутизатори. Його можна використовувати з апаратними прискорювачами шифрування для підвищення продуктивності.
- SSL VPN дозволяє користувачам підключатися до пристроїв VPN за допомогою веб-браузера. Протокол SSL (Secure Sockets Layer) або протокол TLS (Transport Layer Security) використовується для шифрування трафіку між веб-браузером та пристроєм SSL VPN. Однією з переваг використання SSL VPN є простота використання, оскільки всі стандартні веб-браузери підтримують протокол SSL, тому користувачам не потрібно завантажувати чи налаштовувати програмне забезпечення.

1.3.1 Мережі VPN рівня 2

У мережі VPN рівня 2 на основі MPLS трафік пересилається граничним комутатором (Customer Edge - CE) або граничним маршрутизатором клієнта на граничний комутатор постачальника послуг (Provider Edge - PE) у форматі рівня 2. Він переноситься за допомогою технології MPLS через мережу постачальника послуг і потім перетворюється назад у формат 2-го рівня в точці отримання.

У VPN рівня 2, маршрутизація відбувається на комутаторах клієнта, як правило, на комутаторі CE [4]. Комутатор CE, підключений до постачальника послуг у VPN рівня 2, повинен вибрати відповідну схему, по якій надсилати трафік. Комутатор PE, що приймає трафік, посилає його через мережу постачальника послуг до комутатора PE, підключеного до точки приймання. PE комутатори не зберігають і не обробляють маршрути замовника; комутатори

повинні бути налаштовані для передачі даних у відповідний тунель. Для VPN рівня 2 клієнти повинні налаштувати власні комутатори, щоб переносити весь трафік 3-го рівня. Постачальник послуг повинен визначити лише те, скільки трафіку потрібно буде переносити VPN рівня 2. Комутатори постачальника послуг передають трафік між точками клієнта, використовуючи VPN-інтерфейси 2-го рівня. Топологія VPN визначається політикою, налаштованою на PE комутаторах.

Клієнти повинні знати лише, які інтерфейси VPN підключаються до якої з їх точок. Рис 1.1 ілюструє повнозв'язну мережу VPN 2-го рівня, в якій кожна точка має VPN-інтерфейс, пов'язаний з кожною іншою точкою клієнтів. У повнозв'язній топології між усіма трьома точками, кожна точка потребує два логічні інтерфейси (по одному для іншого маршрутизатора або комутатора CE), хоча для підключення PE комутатора до кожного маршрутизатора або комутатора CE потрібна лише одна фізична лінія.

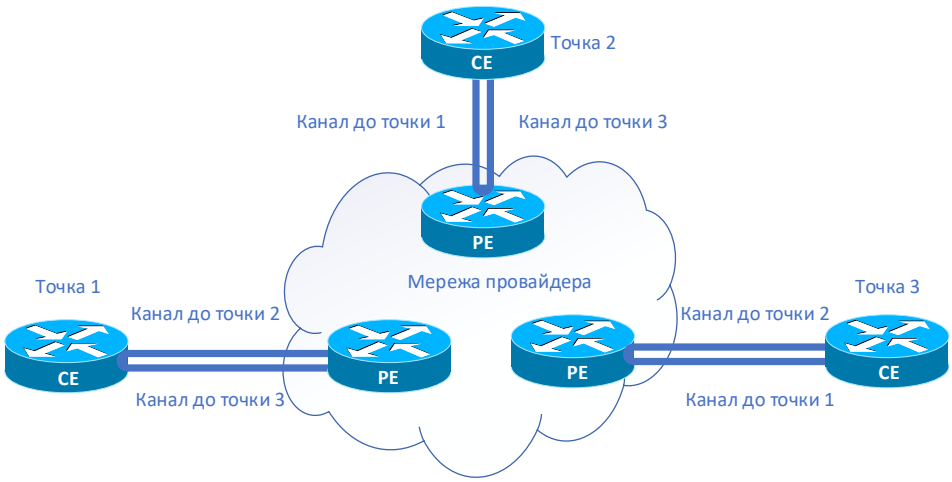

Рисунок 1.1 – Повнозв'язна мережа VPN 2-го рівня

1.3.2 Мережі VPN рівня 3

У VPN рівня 3, маршрутизація відбувається на маршрутизаторах постачальника послуг (PE). Тому VPN 3 рівня потребує більшої конфігурації з боку постачальника послуг, оскільки PE маршрутизатори постачальника послуг

повинні зберігати та обробляти маршрути клієнта. VPN 3-го рівня базуються на RFC 4364, BGP/MPLS IP. Цей RFC визначає механізм, за допомогою якого постачальники послуг можуть використовувати свої IP-магістралі для надання послуг VPN рівня 3 для своїх клієнтів. Точки, що складають VPN рівня 3, підключені через існуючу загальнодоступну мережу Інтернет-провайдера.

Клієнтські мережі, оскільки вони є приватними, можуть використовувати або загальнодоступні, або приватні адреси, визначені в RFC 1918. Коли мережі клієнтів, які використовують приватні адреси, підключаються до загальнодоступної Інтернет-інфраструктури, приватні адреси можуть перетинатися з приватними адресами, якими користуються інші користувачі мережі. BGP/MPLS VPN вирішують цю проблему, додаючи ідентифікатор VPN до кожної адреси з певної точки VPN, тим самим створюючи адресу, унікальну як у VPN, так і в загальнодоступному Інтернеті (табл 1.1).

Таблиця 1.1 - Порівняння мереж VPN другого і третього рівня

VPN рівня 2	VPN рівня 3
Точки клієнтів знаходяться в одній локальній мережі, навіть якщо вони географічно віддалені.	Технічна експертиза постачальника послуг забезпечує ефективну маршрутизацію від точки до точки. Постачальники послуг можуть надавати послуги з доданою вартістю, що включають в себе голос, відео та дані.
Постачальник послуг не потребує інформації про мережеву топологію, політику, інформацію про маршрутизацію клієнта тощо. Замовник має повний контроль над політиками та маршрутизацією.	Клієнти повинні ділитися інформацією про топологію своєї мережі. Постачальник послуг визначає політики та маршрутизацію.

Продовження таблиці 1.1

Комутатор клієнта спрямовує трафік на комутатор постачальника послуг у форматі 2-го рівня.	Комутатор CE клієнта повинен бути налаштований на використання BGP або OSPF для зв'язку з комутатором постачальника послуг PE для передачі IP-префіксів по всій мережі. Інші пакети протоколів не підтримуються.

1.3.3 Технологія MPLS VPN

Віртуальна приватна мережа, що працює за технологією Multiprotocol Label Switching (MPLS) складається з набору точок, які пов'язані між собою за допомогою основної мережі (ядра) провайдера MPLS. На кожній точці замовника один або більше граничних маршрутизаторів клієнта (CE) приєднуються до одного або декількох крайових маршрутизаторів провайдера.

Звичайні VPN створюються шляхом налаштування повної сітки тунелів або постійних віртуальних схем (ПВС) до усіх точок у VPN. Цей (MPLS) тип VPN непростий у обслуговуванні чи розширенні, оскільки додавання нової точки потребує змін кожного граничного пристрою у VPN. VPN на основі MPLS створюються на рівні 3 та базуються на одноранговій моделі. Однорангова модель дозволяє постачальнику послуг та замовнику обмінюватися інформацією про маршрут 3-го рівня. Постачальник послуг ретранслює дані між клієнтськими точками без участі замовника. MPLS VPN простіше керувати та розширювати, ніж звичайні VPN. Коли нова точка додається до MPLS VPN, має бути лише оновлено конфігурацію граничного маршрутизатора провайдера, що надає послуги точці клієнта.

Структурно MPLS VPN (рис 1.2) може бути описано наступним чином [5]:

- Маршрутизатор провайдера (P) - Маршрутизатор в ядрі мережі провайдера. P маршрутизатори виконують комутацію MPLS і не прикріплюють мітки VPN (мітка MPLS у кожному маршруті надається маршрутизатором PE – граничним маршрутизатором провайдера) до маршрутизованих пакетів. VPN Мітки використовуються для направлення пакетів даних до правильного маршрутизатора виходу.
- PE маршрутизатор (граничний маршрутизатор провайдера) - маршрутизатор, який прикріплює мітку VPN до вхідних пакетів на основі інтерфейсу або підінтерфейсу, за яким вони отримані. Маршрутизатор PE приєднується безпосередньо до маршрутизатора CE.
- Маршрутизатор клієнта (C) - Маршрутизатор у мережі провайдера або у корпоративній мережі.
- Граничний маршрутизатор клієнта (CE) - крайовий маршрутизатор у мережі провайдера, що підключається до мережі маршрутизатора PE. Маршрутизатор CE повинен взаємодіяти з маршрутизатором PE.

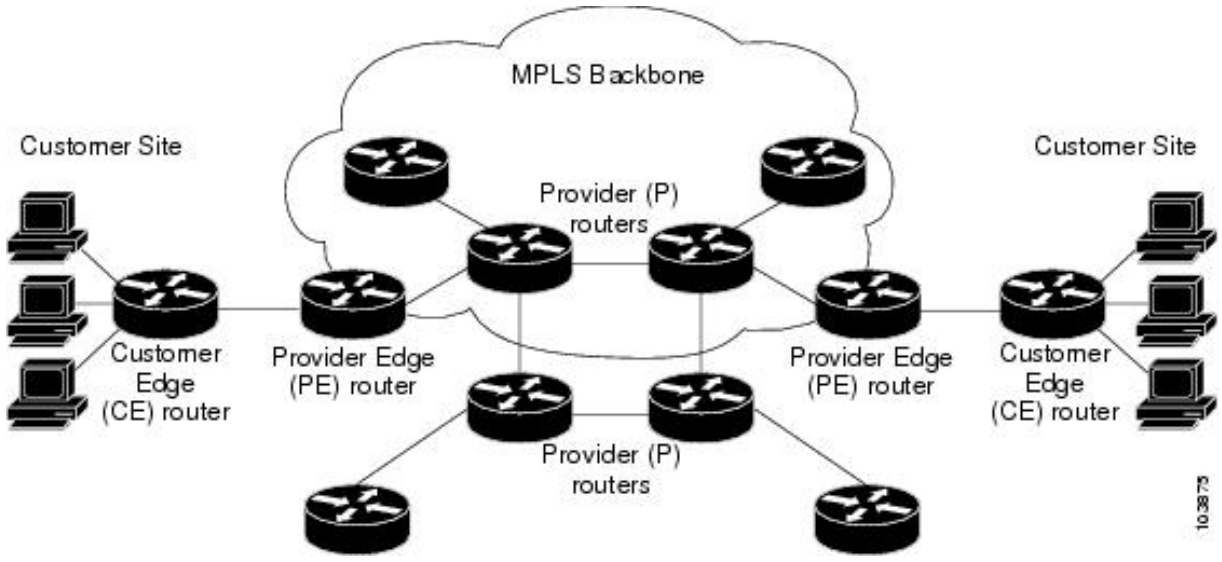

Рисунок 1.2 - базова MPLS VPN

Опишемо принцип роботи MPLS VPN. Функціонал MPLS VPN діє на границі мережі MPLS. Граничний маршрутизатор провайдера - PE виконує наступні функції :

- Обмінюється маршрутизаційними оновленнями з граничним маршрутизатором клієнта – CE;
- Переводить інформацію про маршрутизацію CE у маршрути VPNv4;
- Обмінюється маршрутами VPNv4 з іншими маршрутизаторами через протокол зовнішньої маршрутизації BGP (MP-BGP).

Таблиці віртуальної маршрутизації та переадресації в VPN MPLS працюють наступним чином:

Кожна VPN асоціюється з одним або кількома екземплярами віртуальної маршрутизації та переадресації (VRF). VRF визначає членство в VPN на точці клієнта, що приєднана до маршрутизатора PE.

VRF складається з наступних компонентів:

- Таблиця маршрутизації IP;
- Таблиця переадресації Cisco Express;
- Набір інтерфейсів, які використовують таблицю переадресації;
- Набір правил і параметрів протоколу маршрутизації, які керують інформацією, що включена до таблиці маршрутизації.

Відносини «один до одного» не обов'язково мають існувати між клієнтськими точками та VPN. Одна точка може бути членом декількох VPN. Однак точка може асоціюватися лише з одним VRF. VRF точка містить усі маршрути, доступні для точки з VPN, учасником якої вона, власне, є.

Інформація про переадресацію пакетів зберігається в таблиці маршрутизації IP та таблиці переадресації Cisco для кожного VRF. Також для кожного VRF підтримується окремий набір таблиць маршрутизації та переадресації Cisco Express. Ці таблиці запобігають передачі інформації за межі VPN, а також запобігають наявності пакетів поза VPN від переадресації до маршрутизатора в межах VPN.

Нижче наведено, як розподіляється інформація про маршрутизацію VPN в MPLS VPN.

Розподіл інформації про маршрутизацію VPN контролюється за допомогою використання цілі маршруту VPN, що поширюється протоколом зовнішньої маршрутизації - BGP. Інформація про маршрутизацію VPN поширюється наступним чином:

- Коли маршрут VPN, визначений маршрутизатором CE, вводиться в BGP, список маршрутизації VPN з розширеними атрибутами стає також пов’язаним з ним. Зазвичай список цільових маршрутів з розширеними атрибутами встановлюються зі списку експорту цільових маршрутів, пов'язаних з VRF, з якого маршрут був визначений.
- Список цілей маршрутизації, призначених для маршруту, пов'язаний із кожним VRF. Список імпорту визначає розширені атрибути цільових маршрутів, які повинен мати маршрут для того, щоб імпортувати його до VRF. Наприклад, якщо список імпорту для певного VRF включає цілі маршруту A, B і C, то будь-який маршрут VPN, який містить будь-яку із цих цілей маршруту - A, B або C - імпортується до VRF.

Пересилання MPLS

На основі інформації про маршрутизацію, що зберігається в таблиці маршрутизації IP VRF та таблиці пересилання VRF Cisco Express Forwarding (CEF), пакети пересилаються до місця призначення за допомогою MPLS.

Маршрутизатор PE прив'язує мітку до кожного префіксу клієнта, визначеного за допомогою маршрутизатора CE, і включає мітку в інформацію про доступність мережі для префікса, який вона пропонує іншим маршрутизаторам PE. Коли маршрутизатор PE пересилає пакет, отриманий від маршрутизатора CE через мережу провайдера, він позначає пакет міткою, яку дізнався від маршрутизатора призначення PE. Коли маршрутизатор призначення - PE отримує пакет з міткою, він «забирає» ярлик і використовує його для направлення пакета до правильного маршрутизатора CE. Переадресація міток через магістраль провайдера базується на динамічному

перемиканні міток або на шляхах трафіку. Пакет даних клієнта несе дві однакові мітки при проходженні магістралі:

- Верхня мітка спрямовує пакет до правильного маршрутизатора PE.
- Друга мітка вказує, як цей маршрутизатор PE повинен переслати пакет до маршрутизатора CE.

Компоненти MPLS VPN

Мережа VPN на основі MPLS має три основні компоненти:

- Сукупність цільових маршрутів VPN - це список усіх членів «VPN громади». Цілі маршруту VPN потрібно налаштувати для кожного члена сукупності VPN.
- Мультипротокольний BGP (MP-BGP) піринг маршрутизаторів PE VPN сукупності - MP-BGP поширює інформацію про доступність VRF для всіх членів сукупності VPN. Піринг MP-BGP повинен бути налаштований на всіх маршрутизаторах PE в межах сукупності VPN.
- Переадресація MPLS - MPLS здійснює транспортування всього трафіку між усіма членами сукупності VPN через VPN мережу постачальника послуг.

Відносини один до одного не обов'язково існують між клієнтськими точками та VPN. Одна точка може бути членом декількох VPN, однак точка може асоціюватися лише з одним VRF. VRF на точці клієнта містить усі маршрути, доступні для цієї точки від VPN, учасником якого вона, власне, є.

Основними перевагами MPLS VPN є наступні:

- сервіс без встановлення з’єднання,
- не потрібні тунелі для шифрування та конфіденційності мережі,
- централізоване обслуговування,
- масштабованість,
- підтримка якості обслуговування (QoS),
- безпека,
- легкість у створенні,

- гнучка адресація,
- пряма міграція.

MPLS VPN дозволяють провайдерам розгортати масштабовані VPN та створювати фундамент для доставки таких послуг з додатковою вартістю, як:
Сервіс без встановлення з’єднання

Важливою технічною перевагою VPN-мереж MPLS є те, що вони – мережі без встановлення з’єднання. Інтернет зобов’язаний своїм успіхом основній технології - TCP/IP. TCP/IP побудовано на мережевій парадигмі на основі пакетів без встановлення з’єднання.

Це означає, що не потрібно жодних попередніх дій для встановлення зв'язку між хостами, що робить його легким для зв’язку обох сторін. Щоб встановити конфіденційність IP-середовища, поточне VPN рішення накладають на мережу, орієнтовану на «точка-точка».

При створенні VPN без встановлення з’єднання більше не потрібні тунелі для шифрування та конфіденційності мережі.
Централізоване обслуговування

Побудова VPN на рівні 3 дозволяє надавати цільові послуги групі користувачів, представлених VPN. VPN повинен надавати постачальникам послуг більше, ніж просто механізм для приватного підключення користувачів до інтрамережі (внутрішньої). Він також повинен забезпечити спосіб гнучкої доставки послуг з доданою вартістю для цільових клієнтів.

Масштабованість є критично важливою, оскільки клієнти хочуть приватно користуватися послугами у своїх інтрамережах (intranet) та екстрамережах (extranet).

Оскільки MPLS VPN розглядаються як приватні інтранети, можна використовувати нові IP-сервіси, такі як:

- Багатоадресна передача;
- Якість обслуговування (QoS);
- Підтримка телефонії в межах VPN;

- Централізовані послуги, включаючи вміст та веб-хостинг для VPN.

Можна налаштувати кілька комбінацій спеціалізованих сервісів для індивідуальних клієнтів. Наприклад, послуга, що поєднує IP-трансляцію з низьким рівнем затримки, забезпечує можливість проведення відеоконференцій у межах інтранет.

Масштабованість

Якщо створюється VPN, використовуючи шляхи, орієнтовані на з'єднання «точка-точка», Frame Relay, ATM віртуального підключення (VC), ключовим недоліком VPN є масштабованість. Зокрема, VPN, орієнтовані на неповнозв’язні з’єднання між точками клієнтів, що не є оптимальними. Натомість VPN на основі MPLS використовують однорангову модель та архітектуру без встановлення з’єднань рівня 3 для використання високомасштабного рішення VPN. Модель вимагає, щоб точка клієнта взаємодіяла лише з одним маршрутизатором PE, на відміну від усіх інших маршрутизаторів клієнтів (CE), які є членами VPN. Архітектура без встановлення з’єднання дозволяє створювати VPN на рівні 3, виключаючи потребу в тунелях або в віртуальному підключенні.

Інші проблеми масштабування MPLS VPN пов'язані з розділенням маршрутів VPN між маршрутизаторами PE та подальшим розподілом маршрутів VPN, та IGP маршрутів між маршрутизаторами PE та маршрутизаторами провайдера (P) в ядрі мережі.

- Маршрутизатори PE повинні підтримувати маршрути VPN для тих VPN, учасниками яких вони є.
- P маршрутизатори (провайдера) не підтримують VPN-маршрути. Це збільшує масштабованість ядра провайдера та гарантує, що жоден пристрій не є слабкою ланкою у масштабуванні.

Безпека

MPLS VPN пропонують той же рівень безпеки, що і VPN, орієнтовані на з'єднання. Пакети з однієї VPN не можуть ненароком потрапити до іншої VPN.

Безпека забезпечується в таких ділянках:

- На границі мережі провайдера, гарантуючи, що пакети, отримані від клієнта, потрапляють у правильну VPN.
- На магістралі трафік VPN зберігається окремо. Зловмисне підроблення (спроба отримати доступ до PE маршрутизатора) майже неможливе, оскільки отримані від клієнтів пакети - це IP-пакети. Ці IP пакети повинні бути отримані на певному інтерфейсі або підінтерфейсі, щоб бути однозначно ідентифікованими за VPN міткою.

Легкість у створенні

Щоб повністю використовувати переваги VPN, клієнти повинні мати можливість легко створювати нові VPN та спільноти користувачів. Можливо додавати точки в інтранети та екстранети та формувати закриті групи користувачів. Керування VPN таким способом дає можливість членства будь-якої точки в декількох VPN, збільшуючи гнучкість у створенні інтранетів та екстранетів.

Гнучка адресація

Щоб зробити послугу VPN більш доступною, клієнти постачальника послуг можуть створити власний план адресації, незалежний від планів адресації для інших клієнтів провайдера. Багато клієнтів використовують приватні адресні простори, визначені в RFC 1918, і не хочуть витрачати час і гроші на перетворення загальнодоступних IP-адрес для забезпечення підключення до інтрамережі. MPLS VPN дозволяють клієнтам продовжувати користуватися своїми адресними просторами без трансляції мережевих адрес (NAT) шляхом надання загальнодоступного та приватного перегляду адреси. NAT необхідний, лише якщо два VPN з адресами, що співпадають, хочуть взаємодіяти. Це дає змогу клієнтам використовувати власні незареєстровані приватні адреси та вільно спілкуватися через систему загальнодоступної мережі IP.

Підтримка якості обслуговування QoS - важлива вимога для багатьох клієнтів IP VPN. Це забезпечує можливість дотримання двох основних вимог VPN:

- Передбачувана ефективність та реалізація політики;
- Підтримка декількох рівнів обслуговування в MPLS VPN.

Мережевий трафік класифікується та маркується на границі мережі до того, як трафік агрегується відповідно до політики, визначеної абонентами та реалізованої провайдером, та передається через ядро провайдера. Потім трафік на границі мережі та ядрі може бути розділений за різними класами: ймовірністю відкидання кадру або затримкою.

Пряма міграція. Для того щоб сервіс-провайдери могли швидко розгортати VPN-служби, необхідно використовували прямий шлях міграції. VPN-адреси MPLS унікальні тим, що дають можливість будувати їх на багатьох мережевих архітектурах, включаючи IP, Frame-Relay, ATM та гібридні мережі.

Міграція для клієнта суттєво спрощується, оскільки немає необхідності у підтримці MPLS на CE маршрутизаторі так само, як і у жодних модифікаціях для внутрішньої мережі клієнта.

1.4 Висновки до розділу 1

У першому розділі визначено, що одним із засобів забезпечення безпеки мережевого трафіку та самих мереж є використання віртуальних приватних мереж (VPN), які застосовують будь-яку комбінацію технологій для захисту з'єднання, тунелювання через незахищену або ненадійну мережу. Надано основні рекомендації щодо створення VPN.

З’ясовано, що технологія VPN призначена для захисту мережевої взаємодії між географічно розподіленими користувачами, може бути реалізована на різних рівнях моделі OSI та виконана у різних реалізаціях, в залежності від необхідного функціоналу, розміру мереж та передбаченого навантаження на них.

Зазначено, що VPN використовують тунелювання за допомогою протоколів IPsec, L2TP, PPTP та SSL, шифрування трафіку для забезпечення конфіденційності даних, аутентифікацію користувача та алгоритми забезпечення цілісності даних.

Наведено класифікацію віртуальних приватних мереж на основі брандмауера, на основі апаратних засобів, на основі програмного забезпечення та SSL VPN і розглянуті їх особливості.

Досліджено мережі VPN рівня 2 і 3 та надана їх порівняльна характеристика. Основними відмінностями VPN рівня 3 є визначення політик та маршрутизації постачальником послуг і необхідність клієнтів ділитися інформацією про топологію своєї мережі. Також комутатор CE клієнта повинен бути налаштований на використання BGP або OSPF для зв'язку з комутатором постачальника послуг.

Проаналізовані особливості функціонування технології MPLS VPN та зазначено, що перевагами цієї технології є сервіс без встановлення з’єднання, непотрібність тунелів для шифрування та конфіденційності мережі, централізоване обслуговування, масштабованість, підтримка якості обслуговування (QoS).

2 ПОБУДОВА VPN МЕРЕЖ

2.1 Варіанти побудови віртуальних приватних мереж

Віртуальні приватні мережі також можуть слугувати і для організації мереж без шифрування, тобто загальнодоступних. Існує низка способів реалізації VPN з використанням таких технологій, як: GRE, SSL, IPsec та ін. Побудова віртуальних приватних мереж включає в себе створення тунелів, що являють собою канали, які сполучають два пристрої. Ними, власне, і передаються дані. Налаштування тунелів - обов'язкова задача мережевого інженера при реалізації VPN. Тунелі поділяються на два типи [6]:

1. Remote Access VPN – тунель сполучає комп'ютер користувача з відповідним програмним забезпеченням та будь-який пристрій, що виконує роль сервера і реалізує підключення клієнтів. Ним може бути маршрутизатор, VPN-концентратор, Cisco ASA і т. п.
2. Site-to-Site VPN – передбачає постійний тунель між двома пристроями (наприклад, маршрутизаторами). Користувачі ж знаходяться у локальних мережах (LAN) і даний спосіб тунелювання не потребує завантаження спеціалізованого програмного забезпечення.

Наведемо приклади використання цих технологій.

Перший тип застосовують, коли необхідно забезпечити підключення віддалених співробітників до корпоративної мережі за допомогою захищеного каналу. В даному випадку, якщо користувач має стабільне інтернет-з'єднання та завантажив відповідне програмне забезпечення – комп'ютер самостійно побудує даний тунель до маршрутизатора компанії.

Другий тип часто використовується за необхідності з'єднання віддалених мереж, наприклад, двох філій або філії з центральним офісом. Роботу зі створення тунелю виконує сам граничний маршрутизатор. Він будує віддалене з'єднання між маршрутизатором з локальної мережі користувача – тунель, отже, співробітник без спеціалізованого програмного забезпечення здатний працювати у локальній мережі офісу.

2.2 Тунелювання трафіку та його роль

У VPN зазвичай застосовуються такі технології тунелювання, як IPSec, PPP, L2TP, SSL VPN, GRE VPN. Нижче наведено особливості кожної з них.

2.2.1 Протокол безпеки IPsec

IPsec (internet protocol security) був розроблений IETF (Internet Engineering Task Force) для безпечної передачі інформації на третьому рівні моделі OSI (мережевому) через загальнодоступну незахищену мережу IP, наприклад Інтернет. IPsec дозволяє системі вибирати та узгоджувати необхідні протоколи безпеки, алгоритм(и) та секретні ключі, які будуть використовуватися для потрібних послуг. IPsec забезпечує базову аутентифікацію, цілісність даних та послуги шифрування для захисту від несанкціонованого перегляду та зміни даних. Він використовує [7] AH (Authentication Header - заголовок аутентифікації) та ESP (Encapsulated Security Payload – Безпека інкапсульованого корисного навантаження) для необхідних послуг. Однак IPsec обмежується лише відправленням IP-пакетів.

Протоколи безпеки для безпеки трафіку

IPsec використовує протоколи AH та ESP для надання служб безпеки:

1. Протокол AH (Authentication Header) забезпечує аутентифікацію джерела та цілісність IP-пакетів, але він не має шифрування [8]. Заголовок AH (рис. 2.1), доданий до пакету IP, містить хеш даних, порядковий номер та інформацію, яка може бути використана для перевірки відправника, забезпечення цілісності даних та запобігання повторним атакам.

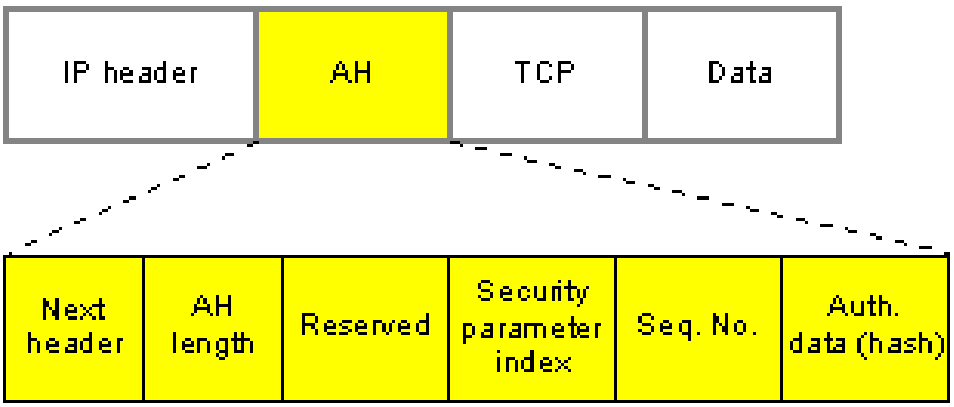

Рисунок 2.1 - Структура заголовка AH

2. Протокол ESP (Encapsulated Security Payload) забезпечує конфіденційність даних додатково до аутентифікації та цілісності. ESP використовує симетричні алгоритми шифрування, такі як 3DES. Алгоритм повинен бути однаковим для обох пристроїв, що комунікують. ESP також може підтримувати конфігурації лише для шифрування або аутентифікації, структуру кадру ESP наведено на рис 2.2. Однак, дослідження 2007 року показали, що будь-які сумісні з RFC реалізації IPsec, які використовують ESP, призначені лише для шифрування, можуть бути зламані.

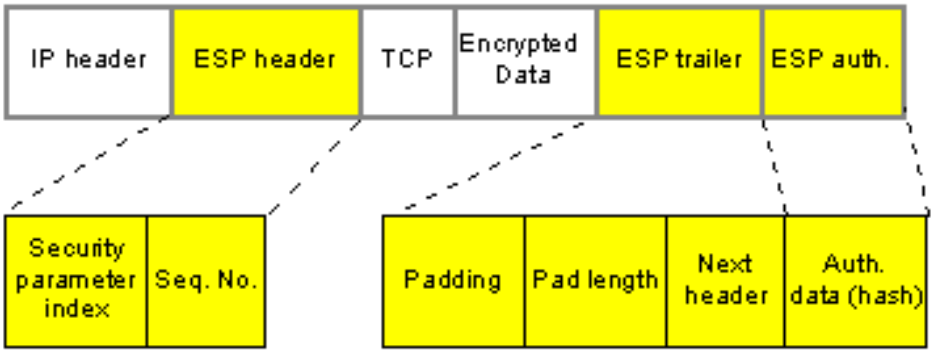

Рисунок 2.2 – Структура кадру ESP

Режими роботи

Кожен протокол безпеки підтримує два режими роботи: режим тунелю та транспортний. Тунельний режим шифрує та/або аутентифікує заголовок та дані

кожного пакету, тоді як режим транспорту шифрує та/або аутентифікує самі дані.

1. Тунельний режим (від кінця до кінця)

В цьому режимі весь пакет захищений. Оригінальний IP-пакет з оригінальною адресою призначення вставляється в новий IP-пакет, а AH і ESP застосовуються до нового пакету (рис. 2.3). Новий IP-заголовок вказує на кінцеву точку тунелю. Після отримання пакету, кінцева точка тунелю буде розшифровувати вміст, а вихідний пакет надалі буде спрямований до кінцевого пункту призначення в цільовій мережі.

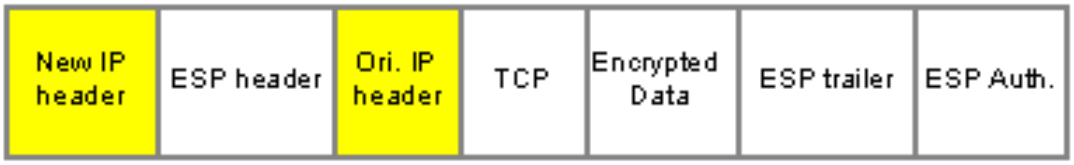

Рисунок 2.3 – Заголовки пакету ESP

2. Режим транспорту (host-to-host)

Тут заголовки AH та ESP застосовуються до даних вихідного пакету IP (рис. 2.4). В цьому режимі шифруються та/або аутентифікуються дані, але не заголовок IP-пакету. Додані накладні витрати менше, ніж потрібно в тунельному режимі. Однак кінцеві адреси призначення та джерела можуть бути викрадені. Зловмисники можуть виконувати аналіз трафіку на основі інформації заголовка в цьому типі заголовка. Зазвичай цей режим використовується лише для з'єднань host-to-host.

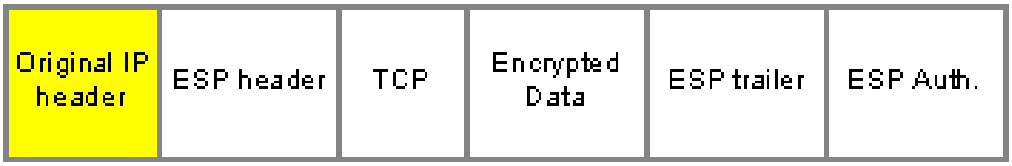

Рисунок 2.4 – Заголовок вихідного пакету

Обмін ключами та управління. IPsec підтримує два типи управління ключами через Інтернет: автоматизований та ручний.

1. Автоматизоване управління ключами IKE (Інтернет-обмін ключами) - це протокол за замовчуванням, який використовується в IPsec для визначення та узгодження протоколів, алгоритмів і ключів, а також для аутентифікації обох сторін. Це корисно для широкомасштабного розгортання та реалізації VPN. Протокол IKEv2 був випущений у 2005 році. Він зберігає більшість функцій протоколу IKEv1, але також підтримує трансляцію мережевих адрес (NAT) та забезпечує більшу гнучкість.

IKE також підтримує використання цифрових сертифікатів. Користувачі аутентифікуються, попередньо підписуючи дані своїм цифровим підписом. Потім інша кінцева точка підтверджує підпис. IKE створює аутентифікований захищений тунель між двома точками, потім узгоджує об'єднання безпеки (SA) між двома об'єктами та обмінюється ключами. SA - це набір параметрів, які використовуються партнерами для переговорів для визначення послуг та механізмів захисту трафіку.

Ці параметри включають ідентифікатори алгоритму, режими, ключі тощо. IKE також відслідковує ключі та оновлює їх під час комунікації клієнтів. IKE використовує такі протоколи, як ISAKMP (Асоціація Інтернет-безпеки та протокол управління ключами) та Oakley для визначення процедур генерації, створення та управління SA та аутентифікації.

Існує кілька методів аутентифікації, де шлюз IPsec VPN працює з IKE для віддаленої аутентифікації користувачів, включаючи гібридну аутентифікацію, розширену аутентифікацію (Xauth), аутентифікацію виклику/відповіді для криптографічних ключів (CRACK) та цифрові сертифікати. Це дозволяє використовувати додаткові сторонні служби аутентифікації для посилення процесу контролю доступу.

2. Ручне управління ключами

Секретні ключі та об’єднання безпеки налаштовуються вручну в обох однорангових комунікаційних VPN перед початком з'єднання. Тільки

відправник та одержувач знають секретний ключ від служб безпеки. Якщо дані аутентифікації дійсні, одержувач знає, що повідомлення надійшло від відправника і не було змінене. Цей підхід простий у використанні в невеликих, статичних середовищах, але він не масштабований. Попередньо всі ключі повинні бути надійно розподілені для спілкування з клієнтами. Якщо ключі скомпрометовано, інша людина може видати себе за користувача та встановити з'єднання з VPN.

2.2.2 Реалізація PPTP з GRE

PPTP (протокол тунелювання з точки на точку) - це протокол канального рівня (OSI), побудований поверх протоколу PPP (протокол точка-точка). PPP - це багатопротокольний комутований протокол, який використовується для підключення до Інтернету. Віддалені користувачі можуть отримати доступ до приватної мережі через PPTP, спочатку дізнавшись IP-адресу у свого локального провайдера. PPTP підключається до цільової мережі, створюючи віртуальну мережу для кожного віддаленого клієнта. PPTP забезпечує сеанс PPP з протоколами, що не належать стеку TCP/IP (наприклад, IP, IPX або NetBEUI), та мають тунелюватися через мережу IP.

Той самий механізм аутентифікації, який використовується для PPP-з'єднань, підтримується у VPN-з'єднанні на основі PPTP. Структуру кадру PPP наведено на рис. 2.5. До них відносяться EAP (протокол поширюваної аутентифікації, MS-CHAP (протокол аутентифікації Microsoft Challenge-Handshake), CHAP, SPAP (протокол аутентифікації пароля Shiva) та PAP (протокол аутентифікації пароля). Шифрування Microsoft "точка-точка-точка", що базується на стандарті RSA RC4 (40/56/128) для шифрування посилання.

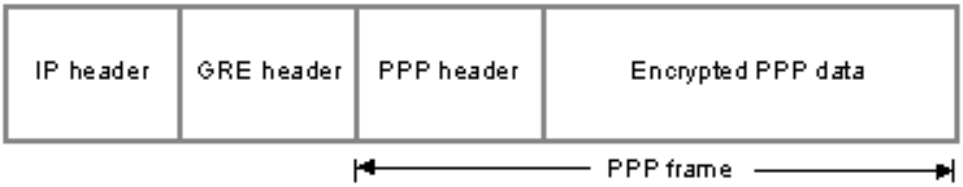

Рисунок 2.5 – Кадр PPP

Тунелювання даних PPTP здійснюється за допомогою декількох рівнів інкапсуляції. PPTP інкапсулює кадри PPP у вигляді тунельних даних для передачі по IP-мережі, наприклад Інтернет або приватний інтранет, використовуючи модифіковану версію GRE (Generic Routing Encapsulation). GRE надає послугу інкапсуляції з контролем потоку та перевантаженості для перенесення пакетів PPP [9]. Дані в інкапсульованих кадрах PPP можуть бути зашифровані (та/або стиснуті).

Отримані в результаті інкапсулювання дані GRE-і-PPP інкапсулюються IP-заголовком, що містить відповідні вихідні та цільові IP-адреси для клієнта PPTP та сервера PPTP. Після отримання тунельованих даних PPTP сервер PPTP обробляє та видаляє заголовки IP, GRE та PPP, після чого розшифровує (та / або розпаковує) дані PPP.

2.2.3 Протокол тунелювання L2TP

L2TP (протокол тунелювання рівня 2) - це комбінація Microsoft PPTP (протокол тунелювання від точки до точки) та Cisco L2F (переадресація рівня 2). L2TP може використовуватися як протокол тунелювання для інкапсуляції кадрів PPP (протокол "точка-точка"), що надсилаються через мережі IP, X.25, Frame Relay або ATM. Дозволено кілька підключень через один тунель. Як і PPTP та L2F, L2TP працює на другому рівні OSI. Два протоколи VPN інкапсулюють дані в межі PPP і здатні передавати протоколи, що не належать до IP, через мережу IP. L2TP задокументовано в RFC 3931.

З'єднання L2TP використовують ті ж механізми аутентифікації, що і PPP-з'єднання, такі як EAP, CHAP, MS-CHAP, PAP і SPAP. Тунелювання L2TP

здійснюється за допомогою декількох рівнів інкапсуляції. Дані PPP інкапсульовані в заголовку PPP та в заголовку L2TP. Інкапсульований пакет L2TP додатково загортається в заголовок UDP з вихідними портами та портами призначення, встановленими на 1701. Остаточний пакет інкапсульований IP-заголовком, що містить вихідні та цільові IP-адреси клієнта VPN та сервера VPN (рис 2.6).

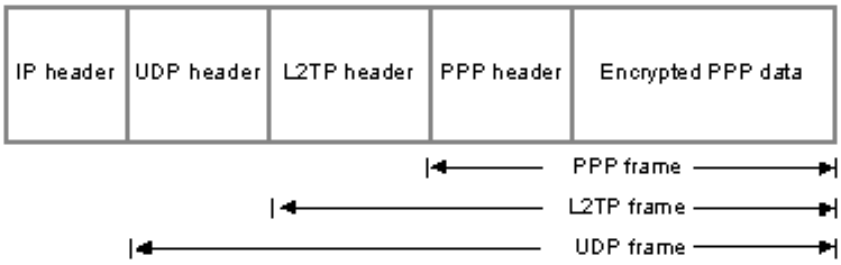

Рисунок 2.6 – Структури кадрів протоколів

Через відсутність конфіденційності, яку надає L2TP, даний протокол часто використовується спільно з IPsec і називається L2TP/IPsec. Коли L2TP працює над IPsec, служби безпеки надаються IPsec, AH та ESP. Усі елементи керування та дані L2TP відображаються як однорідні пакети даних IP до системи IPsec.

2.2.4 Протокол транспортного рівня SSL/TLS

SSL/TLS - протокол транспортного рівня, який використовує порт TCP 443. Протокол SSL визначається IETF, і версії SSL за версією 3.1 немає. TLS 1.0 і TLS 1.1 - це дві стандартизовані версії TLS, а TLS 1.0 - це те саме, що і SSL 3.1. Є ряд криптографічних функцій, що надаються SSL/TLS, і вони включають конфіденційність, цілісність та цифровий підпис [10]. На відміну від IPsec, в якому дві комунікаційні сторони погоджуються на криптографічні функції, SSL/TLS використовує набір шифрів для визначення набору криптографічних функцій, які клієнт і сервер використовують під час спілкування.

Шлюз SSL VPN може аутентифікувати себе веб-користувачеві за допомогою сертифіката сервера SSL, підписаного довіреною службою CA (Центр сертифікації), щоб користувач міг перевірити, чи спілкується він із довіреним сервером через свій браузер. На практиці деякі SSL VPN можуть використовувати цифровий сертифікат, що підписується самостійно, якому зазвичай не довіряють у більшості веб-браузерів. У цьому випадку користувачеві може знадобитися додати серверний сертифікат SSL VPN до власного списку надійних сертифікатів або обрати варіант „так“, щоб довірити сертифікат.

2.3 Висновки до розділу 2

У даному розділі пояснені основні технології тунелювання, визначені принципи їх роботи, призначення та сфери застосування у віртуальних приватних мережах. Було проаналізовано основні реалізації VPN: Remote Access – для зв’язку між географічно розподіленими філіями та Site-to-Site – для доступу користувачів до ресурсів корпоративної мережі з віддалених робочих місць.

На розглянутих у розділі детальних структурах кадрів показано, що підвищення безпеки при передачі даних у VPN без значного додаткового навантаження на обладнання досягається шляхом додавання специфічних заголовків кадру. Перетворення даних у кадрі при цьому не відбувається.

Особливу увагу приділено протоколу IPsec як базі для функціонування захищених з’єднань, його принцип обміну ключами, аутентифікацію та режими роботи.

У зв’язку зі зростаючими вимогами до безпеки та цілісності даних, що ставляться не тільки до великих корпоративних мереж, а й до підключень звичайних користувачів, реалізація VPN з обов’язковим використанням протоколів безпеки стає критично необхідною.

3 СТВОРЕННЯ ЕКСПЕРИМЕНТАЛЬНОГО СТЕНДУ

3.1 Вимоги до обладнання

Для створення експериментального стенду необхідно підібрати обладнання, програмне забезпечення та матеріали, які б відповідали наступним вимогам:

- Обов’язкова підтримка всіх функцій Cisco VPN, шифрування та безпеки;
- Підтримка маршрутизаторами операційної системи Cisco IOS не нижче версії 15;
- Здатність системних блоків до створення тунелів VPN за допомогою програми Cisco VPN Client, Cisco Security Device Manager (SDM);
- Компактність, малошумність та енергоефективність обладнання.

Виходячи з цього, а також з точки зору економічної доцільності, вирішено вибрати наступне обладнання (табл. 3.1):

Таблиця 3.1 – Специфікація обладнання

№	Артикул	Опис	К-ть
1	Cisco Catalyst 3750-48PS-S	Стекований комутатор 3-го рівня, 48 портів 10/100, з живленням PoE, 4 гігабитних аплінка, 16 FL/128 DR	1
2	Cisco Catalyst 3560-48TS-S	Комутатор 3-го рівня, 48 портів 10/100, 4 гігабітних аплінка, 32 FL/128 DR	1
3	Cisco 2811	Модульний маршрутизатор з двома портами 10/100Mbps, 4 слотами HWIC, одним слотом NM, NME, двома USB, 64 FL/256 DR	1
4	AIM-VPN/SSL-2	Модуль пришвидшення шифування DES, 3DES, AES та стиснення даних. Підтримує Cisco IOS WebVPN (SSL) termination, IPv6 IPsec, Cisco IOS Secure Multicast (GDOI), DES, 3DES, AES (256), Layer 3 compression (IPPCP), hashing, key exchange, and SA storage (73-1049-02 A0)	1
5	WIC-2T	Синхронний модуль формата WIC (WAN Interface Card) на 2 послідовних порта до 2,048 Mbps	1
6	2811 flash upgrade	Модуль розширення пам'яті 64MB to 1GB flash upgrade	1
7	2811 SDRAM upgrade	Модуль розширення пам'яті 256MB to 512MB SDRAM upgrade	1

Продовження таблиці 3.1

8	Cisco 1841	Модульний маршрутизатор з двома портами 10/100Mbps, 4 слотами HWIC, одним USB, 32 FL/256 DR	3
9	WIC-2T	Синхронний модуль формата WIC (WAN Interface Card) на 2 послідовних порта до 2,048 Mbps	4
10	AIM-VPN/SSL-1	Модуль пришвидшення шифування DES, 3DES, AES та стиснення даних. Підтримує Cisco IOS WebVPN (SSL) termination, IPv6 IPsec, Cisco IOS Secure Multicast (GDOI), DES, 3DES, AES (256), Layer 3 compression (IPPCP), hashing, key exchange, and SA storage (73-1049-02 A0)	3
11	HWIC-4ESW	Модуль Cisco HWIC-4ESW, 4x10/100	3
12	1841 flash upgrade	Модуль розширення пам'яті 32MB to 64MB flash upgrade	3
13	1841 SDRAM upgrade	Модуль розширення пам'яті 128MB to 256MB SDRAM upgrade	3
14	Itona TC7221-S202D	Системний міні-блок (тонкий клієнт) VIA Eden 1000 Ram 2Gb, flash hdd 2Gb, 1xGigabitEthernet, 4xUSB, VGA, DVI, 2xCOM	2
15	Planet KVM-200	KVM-комутатор, на 2 системних блока	1
16		Кабель для KVM. 1xVGA, 1xkeyboard, 1xmouse	2
Кабелі та додаткове обладнання			
17	Cisco CAB-SS-2626X-3	Кабель для зв'язку між маршрутизаторами Cisco Smart Serial Male DTE to Male DCE 3ft	4
18	GLC-T	Гігабитний "мідний" трансивер SFP 1000BASE-T	2
19	UTP patch cable, cat.5e	Патч-корд категорії 5E	4
20		Кабель живлення	8
21	CAB-CONSOLE-RJ45	Консольний кабель Cisco RJ45 на Rs232 DB9 COM Port	4
22	C3KX-RACK-KIT	Стійкове кріплення для комутаторів Cisco 3750/3560 Series (1RU) Rack Mount Kit	2
23	ACS-1841-RM-19	Стійкове кріплення для маршрутизатора Cisco 1841. Cisco ACS-1841-RM-19 Rack mount kit (for the cisco 1841)	3
24	ACS-2811RM-19	Стійкове кріплення для маршрутизатора Cisco 2811. Cisco 2811 Router 19" Rack Mount Kit	1
25		Блок розеток 19", 8 гнізд	1
26		Міні-стійка 19", 9U	1
27		Джерело безперебійного живлення	1
28		Перехідник для консольного кабеля USB-RS232	1

Активне мережеве обладнання цілком відповідає навантаженню, що створюється експериментальними реалізаціями різних типів рішень віртуальних приватних мереж (табл. 3.2 і 3.3).

Таблиця 3.2 - Продуктивність маршрутизаторів

Платформа	Швидкість комутації		Fast/CEF комутація	
	Пакетів в секунду	Mbps	Пакетів в секунду	Mbps
Cisco 1841			75 000	38.40
Cisco 2811	3 000	1.536	120 000	61.44

Таблиця 3.3 - Основні технічні дані активного обладнання

	Маршрутизатор Cisco 1841	Маршрутизатор Cisco 2811	Комутатор Cisco Catalyst 3750-48PS-S	Комутатор Cisco Catalyst 3560-48TS-S	Міні-системний блок Itona TC7221-S202D
Пам’ять DRAM	256 MB (Default: 128 MB)	512 MB (Default: 256 MB)	128 MB	128 MB	2 GB
Пам’ять Flash	64 MB (Default: 32 MB)	1 GB (Default: 256 MB)	16 MB	32 MB	2 GB
Порти USB	1	2			4
Порти LAN	2x10/100	2x10/100	48x10/100	48x10/100	1x10/100/1000
Слоти розширення для Interface Card	2 слоти, кожен пітримує типи модулів HWIC, WIC, VIC, або VWIC (тільки для даних)	4 слоти, кожен пітримує типи модулів HWIC, WIC, VIC, або VWIC			
Слоти розширення для Network-Module		1 слот для NM та NME модулів	4 слоти SFP для оптичних чи мідних гігабітних модулів	4 слоти SFP для оптичних чи мідних гігабітних модулів	

Продовження таблиці 3.3

Голосові PVDM (DSP) слоти вбудовані		2			
Вбудована підтримка VPN, шифрування та безпеки	DES, 3DES, AES 128, AES 192, and AES 256		VLAN, SSH, ACL, QoS, MAC-filtering, TACACS+, RADIUS		
Консольний порт (до 115.2 kbps)	1	1	1	1	2xCOM
Auxiliary порт (до 115.2 kbps)	1	1	1	1	
Операційна система	Cisco IOS 15.1-4 Advanced IP Services K9	Cisco IOS 15.1-4 Advanced IP Services K9	Cisco IOS 12.3 IP Services K9	Cisco IOS 12.3 IP Services K9	Windows
Споживана потужність типова	50W	160W	89W	45W	30W
Вага	2,7 кг	6,4 кг	6,0 кг	6,4 кг	2,5 кг
Розміри (в х ш х г), мм	44.0 x 343 x 274	44.5 x 438.2 x 417	44.0 x 445 x 378	44.0 x 445 x 300	50 x 265 x 245

Для організації компактного розташування та всебічного доступу, було створено рухому телекомунікаційну 9U-стійку зі стандартним розміром кріплень 19”, блоком розподілення живлення та пристроєм безперебійного живлення (ПБЖ).

У межах стенду, для емуляції зв’язку між віддаленими офісами, доцільно використовувати модулі WIC (WAN Interface Card), що забезпечують з’єднання через послідовні порти, наприклад, модулі WIC-2T з відповідними інтерфейсними кабелями.

При виборі інтерфейсних модулів особливу увагу слід приділяти сумісності модулів з однотипним обладнанням, але різних серій. За допомогою

відповідних інтернет сервісів Cisco можна побачити, наприклад, що однакові за функціями та способами установлення модулі AIM-VPN/SSL підтримуються лише у межах однієї серії маршрутизаторів, тому є AIM-VPN/SSL-1 для Cisco 1841 та AIM-VPN/SSL-2 для Cisco 2811.

Також, незважаючи на фізичну сумісність, наприклад, голосових модулів VWIC, вони не будуть функціонувати у Cisco 1841, але будуть у Cisco 2811.

Так само й у випадку з комутаторами. SFP-слоти для гігабітних модулів у різних серіях комутаторів підтримують різні модулі, незважаючи на їх однакові фізичні розміри та вигляд. Виходячи з цього, для комутаторів були обрані гігабітні мідні модулі GLC-T - Гігабітний "мідний" трансивер SFP 1000BASE-T. Також були успішно протестовані й оптичні модулі SFP 100Base-SX.

Таким чином, схема експериментального стенду має наступний вигляд (рис. 3.1).

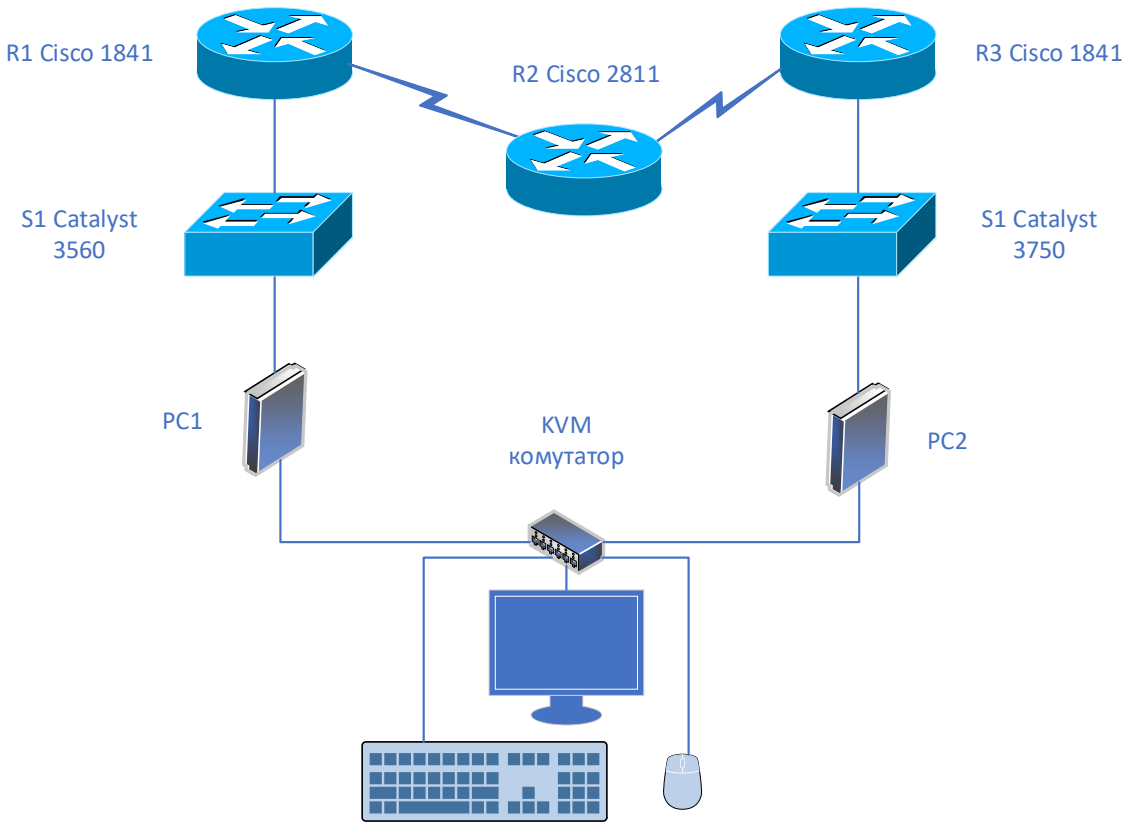

Рисунок 3.1 – Схема експериментального стенду

Ядром стенду слугують маршрутизатори Cisco 1841 та Cisco 2811 (рис. 3.2) з наступними можливостями для підключення (табл. 3.4).

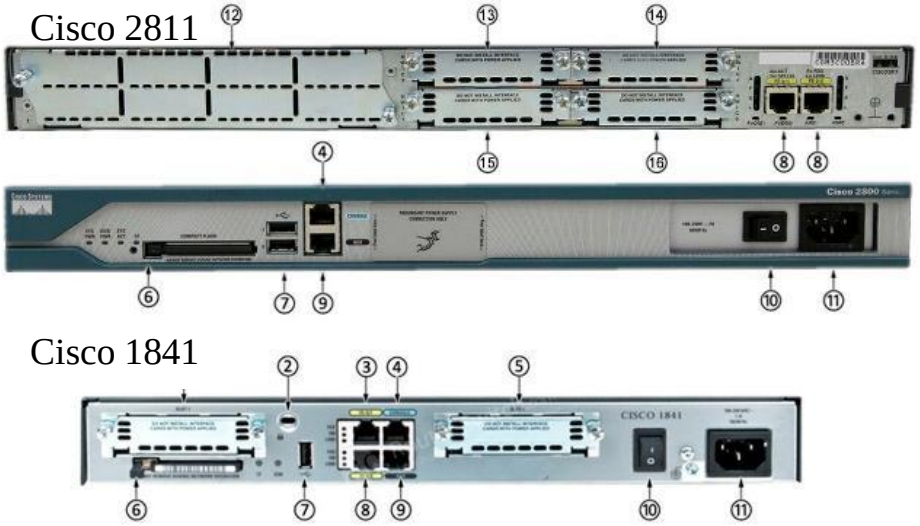

Рисунок 3.2 – Маршрутизатори та їх підключення

Таблиця 3.4 – Конструктивні елементи маршрутизаторів

(1, 5, 13-16)	Слот розширення для модулів WIC, VWIC (data only для Cisco 1841), або HWIC	(7)	USB порти
(2)	Кріплення для замка Kensington Security Slot	(9)	Порт для керування Aux port
(3, 8)	Порти Fast Ethernet ports та LEDs	(10)	Вимикач живлення
(4)	Консольний порт	(11)	Гніздо живлення
(6)	Слот для карти пам’яті CompactFlash memory card slot	(12)	Слот розширення для модулів NM

Після монтажу та налагодження, стенд виглядає наступним чином (рис.3.3).

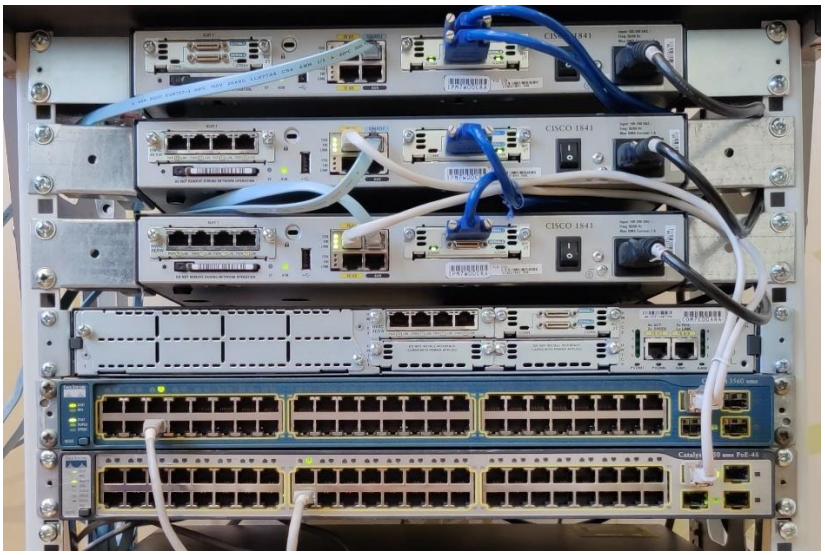

Рисунок 3.3 – Розташування обладнання експериментального стенду

Для сценарію Remote Access, VPN-тунелі створюються за допомогою міні-системних блоків Itona TC7221, об’єднаних KVM-комутатором Planet KVM-200 (рис. 3.4). Також за допомогою цих системних блоків та інстальованої на них програми PuTTY, проводиться конфігурування активного обладнання через інтерфейс командної лінії.

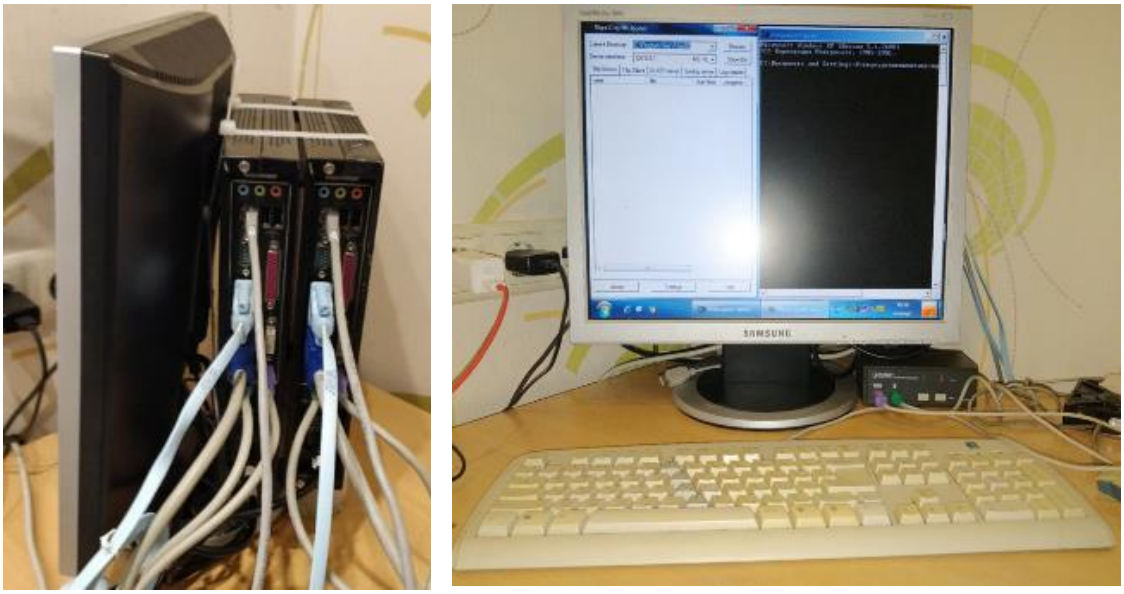

Рисунок 3.4 – Розташування системних міні-блоків Itona та KVM-комутатора

3.2 Вибір типу операційної системи

Виходячи з додаткових вимог до обладнання, з точки зору підтримуваних розширених функцій для забезпечення віртуальних приватних мереж, криптування та безпеки, необхідно підібрати таку версію Cisco IOS (табл. 3.5), яка б задовольняла всім цим вимогам.

Таблиця 3.5 - Список Cisco IOS версії 15

Версія Cisco IOS ревізії 15	Базова передача даних	Голос по IP	ATM та MPLS	Запобігання вторгненням (IPS), Фільтри та шифрування	Міжмережевий екран, IPS для SSL VPN, NAC, DMVPN та Easy VPN	Протокол SSH, HTTPS, SNMPv3
Базова (IP Base)	X					
IP Base без криптографії	X					
Для підприємств (Enterprise)	X			X		X
Для великих підприємств, без криптографії	X			X		
Голосова (IP Voice)	X	X				X
Голосова без криптографії	X	X				
З підвищеною безпекою (Advanced Security)	X				X	X
Для ISP	X	X	X			X
З розширеними функціями (Advanced IP Services)	X	X	X		X	X
Розширена, для великих підприємств, без криптографії	X	X	X	X		
Розширена, для великих підприємств	X	X	X	X		X
Максимальна, для великих підприємств	X	X	X	X		X

Узагальнюючи таблицю 3.5, можна виділити чотири основних типи версій Cisco IOS за функціональністю:

- Base: базовий рівень;
- Services: додатковий сервіс для різних типів IP-телефонії, MPLS;
- Advanced: підтримка VPN, шифрування 3DES, міжмережевого екрану, SSH, протоколу безпеки Cisco IOS IPsec та системи виявлення вторгнень;
- Enterprise: підтримка протоколів для великих підприємств: IBM, AppleTalk, IPX.

Як видно з таблиці 3.5, максимальний набір необхідних функцій (VPN, безпека, криптування) має версія «З розширеними функціями (Advanced IP Services)». На рисунку 3.5 зображено місце даної версії у загальній ієрархії:

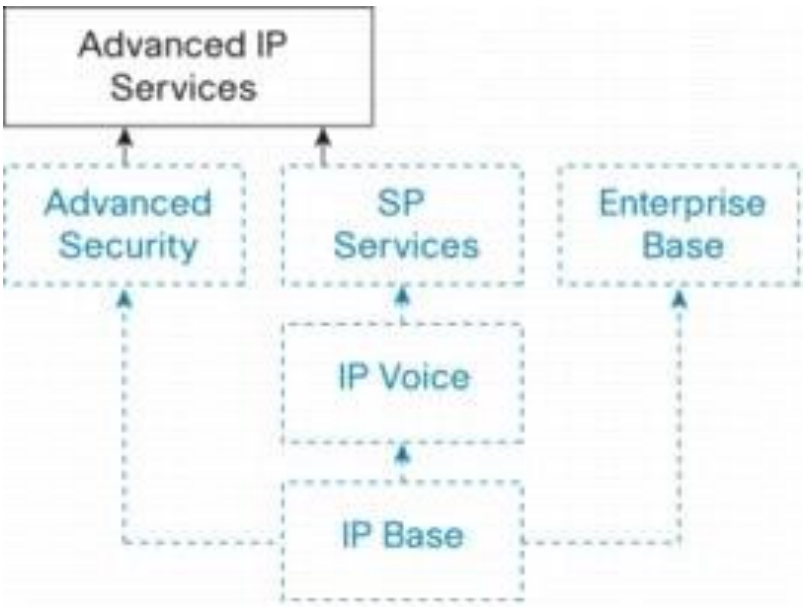

Рисунок 3.5 – Місце Advanced IP Services у ієрархії версій IOS

Однак, використання версії Cisco IOS Advanced IP Services накладає додаткові вимоги щодо ресурсів обладнання. Зокрема, обов'язковим є розширення обсягу пам'яті – Flash та DRAM (табл. 3.6). Для визначення необхідних обсягів треба звернутися до сервісу Cisco Feature Navigator за посиланням: https://cfnng.cisco.com/archived-data .

Таблиця 3.6 – Версії IOS та мінімальний обсяг пам’яті, що потребується

Advanced IP Services для:	Назва образу ОС	Мінімальний обсяг FLASH-пам’яті	Мінімальний обсяг DRAM-пам’яті
Cisco 1841	c1841-advipservicesk9-mz.151-4.M12a.bin	64MB	192MB
Cisco 2811	c2800nm-advipservicesk9-mz.151-4.M12a.bin	128MB	512MB

Використовуючи керівництво з технічного обслуговування для Cisco 1841 та Cisco 2811, були обрані відповідні модулі пам’яті DRAM та виконано апгрейд. Більш складним є процес розширення FLASH-пам’яті, оскільки вона має бути спеціально відформатована. Крім того, вона має містити обраний образ Cisco IOS. Копіювання образу на FLASH-пам’ять може бути виконано наступними методами:

1. Копіювання з USB-Flash командою copy usbflash0: flash: , з подальшим зазначенням точної назви образу ОС;
2. Установка та налаштування tftp-серверу на комп’ютер, налагоджування ip-адрес мережевих інтерфейсів комп’ютера та маршрутизатора так, щоб вони були в одній підмережі, з однаковим шлюзом за замовчуванням. Використовується команда copy tftp: flash: , з подальшим зазначенням точної назви образу ОС;
3. Копіювання образу через перехідник USB-CompactFlash;
4. За допомогою прямого підключення через Xmodem.

Найпростіше використовувати перший або третій метод. Найдовший, але найнадійніший – четвертий. Якщо немає можливості використання USB-Flash або CompactFlash перехідника, то найбільш вживаним є другий метод. Також, другий метод має додаткові переваги, оскільки найбільш поширена програма для його використання, tftpd32, дозволяє налаштовувати як DHCP, TFTP, так і

SNTP сервери, вести ще й логування процесів на сервері Syslog, що й було використано в даній роботі.

Маючи офіційну реєстрацію у системі Cisco та відповідний статус, дані образи ОС можна отримати за запитом до виробника.

3.3 Висновки до розділу 3

Даний розділ присвячено створенню та налаштуванню експериментального стенду, на якому відпрацьовано методи реалізації всіх основних типів VPN-тунелювання та захищеного доступу. Крім того, в процесі створення стенду були здобуті наступні навички:

- Ознайомлення зі спектром комутаторів та маршрутизаторів Cisco, які б ефективно та економічно доцільно могли б бути використані у домашній лабораторії;
- Вивчення особливостей різних версій Cisco IOS та визначення оптимальної для налаштування віртуальної приватної мережі з відповідними шифруванням та безпекою;
- Механічного монтажу, підключення, з’єднань та апгрейду обладнання. Правильного вибору обладнання з точки зору функціоналу, енергоефективності та малошумності;
- Вибору та установки програмного забезпечення з використанням сервісів та документації від Cisco.

4 НАЛАШТУВАННЯ VPN НА ОБЛАДНАННІ ФІРМИ CISCO

4.1 Налаштування Site-to-Site VPN з використанням технології тунелювання IPsec

Традиційні методи створення тунелів між територіально віддаленими мережами, наприклад, за допомогою технологій MPLS чи GRE, забезпечують лише передавання трафіку між мережами, але не підтримують достатній для сучасних вимог рівень безпеки, а саме, відсутні функції шифрування, розширені методи аутентифікації та політики безпеки. Можливо уникнути усіх цих недоліків при використанні технології тунелювання IPsec.

Тому основну увагу у даному пункті роботи приділено методу створення саме IPsec тунелів. Ця технологія підтримується усіма основними виробниками активного обладнання. До того ж, на базі цієї технології та обладнання тільки від Cisco Systems, можливо реалізувати найбільш сучасні методи створення захищених тунелів, такі як:

- Cisco IPSec VTI (Віртуальний Тунельний Інтерфейс) – це технологія створення віртуальних інтерфейсів для маршрутизації зашифрованих тунелів IPsec. Весь трафік в такому тунелі автоматично підлягає шифруванню, при цьому конфігурування пристроїв значно спрощується;
- Dynamic Multipoint VPN – також підтримує статичну та динамічну маршрутизацію. Особливістю є можливість динамічного встановлення тунелю при підключенні нових віддалених мереж;
- Flex VPN – це найбільш універсальна технологія від Cisco, за допомогою якої всі типи тунелів конфігуруються однаково. До того ж, важливою перевагою даної технології є автоматичний захист VPN мережі від DDoS-атак. Технологія сумісна з мережами VPN, побудованими на обладнанні інших виробників.

Саме тому в даному пункті розглянуто налаштування IPsec VPN як основу всіх сучасних методів захищеного тунелювання.

У цій частині дипломної роботи буде побудована та налаштована мережа з декількома маршрутизаторами, використана Cisco IOS для налаштування VPN реалізації Site-to-Site, а потім - тестування VPN.

Тунель VPN IPsec проходить від R1 до R3 через R2 (рис. 4.1, табл. 4.1). R2 діє як «прохідний» маршрутизатор і не знає про VPN. IPsec забезпечує безпечну передачу конфіденційної інформації через незахищені мережі, наприклад Інтернет.

IPsec діє на мережевому рівні, захищає та аутентифікує IP-пакети між учасниками IPsec-пристроїв (одноранговими), такими як маршрутизатори Cisco.

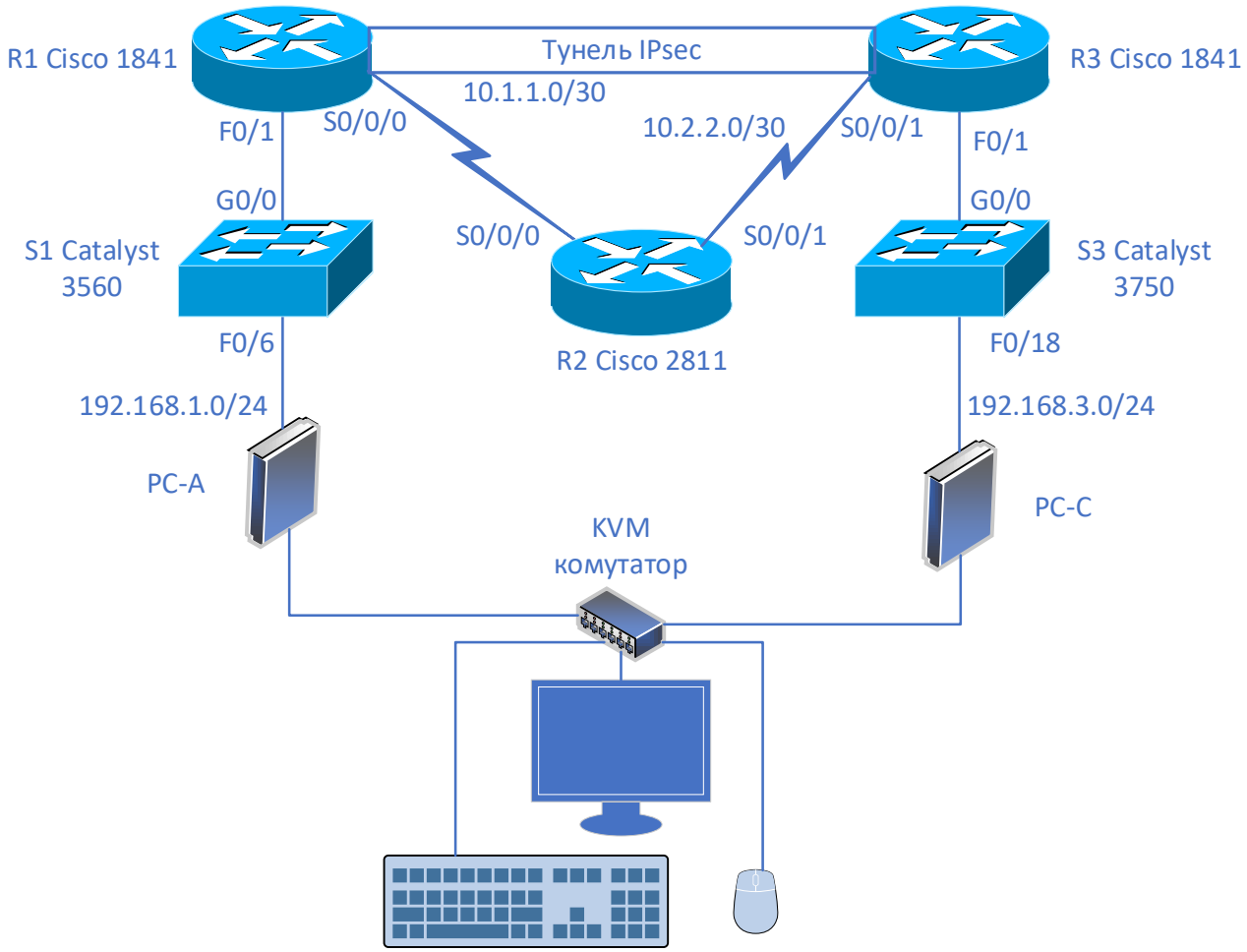

Рисунок 4.1 – Тополія мережі для реалізації Site-to-Site VPN

Таблиця 4.1 – IP-адресація

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Порт комутатора
R1	F0/1	192.168.1.1	255.255.255.0	N/A	S1 G0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	F0/1	192.168.3.1	255.255.255.0	N/A	S3 G0/0
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Цілі:

Частина 1: Базове налаштування пристроїв

• Налаштування імен хостів, IP-адрес інтерфейсів та паролів доступу.

• Налаштування протоколу маршрутизації OSPF.

Частина 2: Налаштування VPN від точки до точки за допомогою Cisco IOS

• Налаштування параметрів IPsec VPN на R1 та R3.

• Перевірка налаштування IPsec VPN від точки до точки.

• Перевірка роботи IPsec VPN.

VPN реалізації Site-to-Site зазвичай забезпечує захищений (IPsec або інший) тунель між філією та центральним офісом. Інша поширена реалізація технології VPN - це віддалений доступ до корпоративного офісу з робочого місця наприклад, невеликого офісу чи домашнього офісу.

Необхідні ресурси:

- 3 маршрутизатори (Cisco 1841 з Cisco IOS версії 15.1 (4) M12A з ліцензією технологічного пакета безпеки – advipservicesk9, Cisco 2811 з Cisco IOS версії 15.1 (4) M12a з ліцензією технологічного пакета безпеки - advipservicesk9)

- 2 комутатори (Cisco 3560-48TS-S та 3750-48PS-S)
- 2 ПК (Windows, програма Putty з терміналом та клієнтом SSH)
- Послідовний (Serial) і Ethernet-кабелі, як показано в топології
- WAN-модулі WIC-2T для зв’язку між маршрутизаторами
- Консольні кабелі для налаштування мережевих пристроїв Cisco

Частина 1: Базове налаштування пристроїв

У частині 1 буде встановлена мережева топологія та налаштовані основні параметри, такі як IP-адреси інтерфейсів, динамічна маршрутизація, доступ до пристроїв та паролі.

Крок 1: Підключення мережі, як показано в топології (рис. 4.1).

Приєднати пристрої та кабелі, як показано на діаграмі топології.

Крок 2: Налаштування основних параметрів для кожного маршрутизатора (табл.4.1).

- Налаштування імен хостів, як показано в топології;
- Налаштування IP-адрес інтерфейсів, як показано в таблиці IP-адресації;
- Налаштування тактової частоти 64000 (clock rate) для послідовних інтерфейсів маршрутизатора із підключеним послідовного кабелю Serial DCE.

Крок 3: Вимкнення пошуку DNS.

Необхідно вимкнути пошук DNS, щоб запобігти спробі маршрутизатора обробити неправильно введені команди.

Крок 4: Налаштування протоколу маршрутизації OSPF на R1, R2 та R3.

1. На R1 мають бути налаштовані наступні команди:

```
R1(config)# router ospf 101
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

2. На R2 мають бути налаштовані наступні команди:

```
R2(config)# router ospf 101
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

3. На R3 мають бути налаштовані наступні команди:

```
R3(config)# router ospf 101
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

Крок 5: Налаштування параметрів IP-адресації клієнтського ПК.

1. Налаштування статичної IP-адресації, маски підмережі та шлюзу за замовчуванням для PC-A, як показано в таблиці IP-адресації.
2. Налаштування статичної IP-адресації, маски підмережі та шлюзу за замовчуванням для PC-C, як показано в таблиці IP-адресації.

Крок 6: Перевірка базового підключення до мережі.

Проведення пінг-запиту від R1 до інтерфейсу R3 Fa0/1 за IP-адресою 192.168.3.1 та від PC-A в локальній мережі R1 до PC-C в локальній мережі R3.

Крок 7: Налаштування та шифрування паролів.

Налаштувати мінімальну довжину пароля. Використати команду "security passwords", щоб встановити мінімальну довжину пароля в 10 символів.

Налаштувати секретний пароль командою enable secret на обох маршрутизаторах паролем cisco12345. Використати алгоритм хешування типу 9 (SCRYPT).

Створити локальний обліковий запис itsvpn61, використовуючи 61itsvpn61 для пароля. Використовувати алгоритм хешування типу 9 (SCRYPT).

Крок 8: Налаштування консольного підключення.

Налаштувати консоль для використання локальної бази даних для входу. Для додаткової безпеки налаштувати лінію для виходу через п’ять хвилин бездіяльності. Використати команду «logging synchronous», щоб не допустити переривання введення команди повідомленнями.

Крок 9: Зберегти основну робочу конфігурацію для всіх трьох маршрутизаторів.

Зберегти поточну конфігурацію до конфігурації запуску у привілейованому режимі EXEC на усіх маршрутизаторах за допомогою команди «copy running-config startup-config».

Частина 2: Налаштування VPN реалізації Site-to-Site за допомогою Cisco IOS

У частині 2 даного алгоритму буде налаштовано тунель VPN IPsec між маршрутизаторами R1 та R3, який проходить через R2. Маршрутизатори R1 та R3 будуть налаштовані за допомогою CLI Cisco IOS. Потім буде проведене тестування конфігурації.

Завдання 1: Налаштування параметрів VPN IPsec на R1 та R3.

Крок 1: Перевірка підключення від локальної мережі R1 до локальної мережі R3. У цьому завданні можна переконатися, що PC-A в локальній мережі R1 може провести пінг-запит до PC-C в локальній мережі R3 без тунелю.

Провести пінг IP-адреси PC-C 192.168.3.3 від PC-A.

```
PC-A:\> ping 192.168.3.3
```

Крок 2: Увімкнути політику IKE на R1 та R3.

IPsec дозволяє обмінюватися протоколами. У реалізації VPN IPsec є два центральних елемента конфігурації:

- Впровадження параметрів IKE (Internet Key Exchange –Обмін Інтернет Ключами);
- Реалізація параметрів IPsec.

1. Перевірити підтримку та роботу IKE

Фаза 1 IKE визначає метод обміну ключами, який використовується для передачі та затвердження політик IKE між користувачами. У фазі 2 IKE користувачі обмінюються і відповідають політикам IPsec для аутентифікації та шифрування трафіку даних. IKE повинен бути включений для функціонування IPsec. За замовчуванням IKE увімкнено для образів IOS із підтримкою криптографічних функцій. Якщо він відключений, можна увімкнути його за допомогою команди crypto isakmp enable. За допомогою цієї команди можна переконатися, чи підтримує IOS маршрутизатора параметри IKE.

```
R1(config)# crypto isakmp enable
R3(config)# crypto isakmp enable
```

2. Встановити політику ISAKMP і переглянути доступні опції.

Щоб дозволити фазу узгодження 1 IKE, необхідно створити політику ISAKMP і налаштувати спільну групу, що включає цю політику ISAKMP. Політика ISAKMP визначає алгоритми аутентифікації та шифрування та хеш-функцію, яка використовується для передачі керуючого трафіку між двома кінцевими точками VPN. Коли політика безпеки зв'язку ISAKMP була прийнята користувачами IKE, етап IKE завершено. Параметри IKE фази 2 будуть налаштовані пізніше.

Ввести команду режиму глобальної конфігурації crypto isakmp policy number на R1 для політики 10.

```
R1(config)# crypto isakmp policy 10
```

3. Переглянути різні параметри IKE, доступні за допомогою довідки Cisco IOS, ввівши знак питання (?).

```
R1(config-isakmp)# ?
ISAKMP commands:   authentication  Set authentication method for
protection suite   default         Set a command to its defaults
encryption      Set encryption algorithm for protection suite   exit
Exit from ISAKMP protection suite configuration mode   group
Set the Diffie-Hellman group   hash            Set hash algorithm for
protection suite   lifetime        Set lifetime for ISAKMP security
association
  no              Negate a command or set its defaults
```

Крок 3: Налаштувати політику ISAKMP фази 1 IKE на R1 та R3. Вибір алгоритму шифрування визначає, наскільки конфіденційним є канал управління між кінцевими точками. Алгоритм хешу контролює цілісність даних, гарантуючи, що дані, отримані від користувача, не підробляються під час передачі. Тип аутентифікації забезпечує, що пакет був відправлений та підписаний віддаленим користувачем. Протокол Діффі-Геллмана використовується для створення секретного ключа, яким обмінюються користувачі, який не надсилався через мережу.

1. Налаштувати політику ISAKMP з пріоритетом 10. Варто використати загальнодоступний ключ – preshared key як тип аутентифікації, AES 256 для алгоритму шифрування, sha як алгоритм хешування та обмін

ключами групи Діффі-Геллмана 14. Потрібно дати політиці час життя 3600 секунд (одну годину).

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 14
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# end
```

2. Налаштувати таку ж саму політику на маршрутизаторі R3:

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# hash sha
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 14
R3(config-isakmp)# lifetime 3600
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# end
```

3. Перевірити політику IKE за допомогою команди show crypto isakmp policy

```
R1# show crypto isakmp policy
Global IKE policy
Protection suite of priority 10         encryption algorithm:   AES - Advanced
Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
authentication method:  Pre-Shared Key          Diffie-Hellman
group:   #14 (2048 bit)
        lifetime:               3600 seconds, no volume limit
```

Крок 4: Налаштування загальнодоступних ключів (pre-shared).

Оскільки попередні спільні ключі використовуються як метод аутентифікації в політиці IKE, ключ повинен бути налаштований на кожному маршрутизаторі, який вказує на іншу кінцеву точку VPN. Для успішної аутентифікації ці ключі повинні співпадати. Для введення заздалегідь відкритого ключа використовується команда режиму глобальної коніфгурації crypto isakmp key <key-string> адреса <ip-address>. Необхідно використовувати

IP-адресу віддаленого однорангового каналу, який є віддаленим інтерфейсом, який би використовувався для передачі трафіку на локальний маршрутизатор.

1. Кожна IP-адреса, яка використовується для налаштування користувачів IKE, також називається IP-адресою віддаленої кінцевої точки VPN. Необхідно налаштувати загальнодоступний ключ sts61 на маршрутизаторі R1. Виробничі мережі повинні використовувати складний ключ. Ця команда вказує на IP-адресу віддаленого однорангового R3 S0/0/1.

```
R1(config)# crypto isakmp key sts61 address 10.2.2.1
```

2. Налаштувати загальнопоширений ключ sts61 на маршрутизаторі R3. Команда для R3 вказує на IP-адресу R1 S0/0/0.

```
R3(config)# crypto isakmp key sts61 address 10.1.1.1
```

Крок 5: Налаштувати набір перетворень і термін служби IPsec.

1. Набір перетворень IPsec (Transform Set) - це ще один параметр конфігурації шифрування, який маршрутизатори узгоджують для формування захищеного зв’язку. Щоб створити набір перетворень IPsec, необхідно використати команду crypto ipsec transform-set <tag>. Використання символу «?» дозволяє побачити, які параметри доступні.

```
R1(config)# crypto ipsec transform-set 50 ?
  ah-md5-hmac   AH-HMAC-MD5 transform   ah-sha-hmac   AH-HMAC-SHA
transform   comp-lzs      IP Compression using the LZS compression
algorithm   esp-3des     ESP transform using 3DES(EDE) cipher (168
bits)   esp-aes        ESP transform using AES cipher   esp-des
ESP transform using DES cipher (56 bits)    esp-md5-hmac   ESP
transform using HMAC-MD5 auth   esp-null       ESP transform w/o
cipher   esp-seal      ESP transform using SEAL cipher (160 bits)
esp-sha-hmac  ESP transform using HMAC-SHA auth
```

2. На R1 і R3 треба створити набір перетворень з тегом 50 і використати перетворення ESP з шифром AES 256 з ESP і хеш-функцією SHA. Набори перетворень повинні співпадати.

```
R1(config)# crypto ipsec transform-set 50 ?
  ah-md5-hmac   AH-HMAC-MD5 transform   ah-sha-hmac   AH-HMAC-SHA
transform   comp-lzs      IP Compression using the LZS compression
algorithm   esp-3des     ESP transform using 3DES(EDE) cipher (168
bits)   esp-aes        ESP transform using AES cipher   esp-des
ESP transform using DES cipher (56 bits)    esp-md5-hmac   ESP
transform using HMAC-MD5 auth   esp-null       ESP transform w/o
cipher   esp-seal      ESP transform using SEAL cipher (160 bits)
esp-sha-hmac  ESP transform using HMAC-SHA auth
```

3. Також можна змінити термін роботи безпечного зв'язку IPsec з 3600 секунд за замовчуванням. На R1 і R3 треба встановити термін роботи безпечного зв'язку IPsec на 30 хвилин або 1800 секунд.

```
R1(config)# crypto ipsec security-association lifetime seconds 1800

R3(config)# crypto ipsec security-association lifetime seconds 1800
```

Крок 6. Визначити важливий трафік.

Для використання шифрування VPN з IPsec необхідно визначити розширені списки доступу, щоб повідомити маршрутизатору, який трафік потрібно шифрувати. Пакет, дозволений списком доступу, який використовується для визначення трафіку IPsec, шифрується, якщо сеанс IPsec налаштований правильно. Пакет, якому відмовлено в одному з цих списків доступу, не відкидається, він надсилається незашифрованим. Також, як і в будь-якому іншому списку доступу, в кінці є неявне заперечення, що означає, що за замовчуванням дія полягає в тому, щоб не шифрувати трафік. Якщо безпека зв'язку IPsec не налаштована правильно, трафік не шифрується, а трафік передається незашифрованим.

У цьому випадку, з точки зору R1, трафік, який потрібно шифрувати, - це трафік, що йде від Ethernet LAN R1 до Ethernet LAN R3 або навпаки, з точки зору R3. Ці списки доступу використовуються на вихідних інтерфейсах кінцевої точки VPN і повинні співпадати.

1. Налаштувати фільтрацію важливого трафіку IPsec VPN на R1.

```
R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

2. Налаштувати фільтрацію важливого трафіку IPsec VPN на R2.

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Крок 7: Створення та застосування криптокарти.

Криптокарта асоціює трафік, який відповідає списку контролю доступу для користувача та різні налаштування IKE та IPsec. Вона складається зі списку контролю доступу, IP-адреси кінцевого користувача, набору перетворень та типу секретності переадресації. Після створення криптокарти її можна застосувати до одного або декількох інтерфейсів. Інтерфейси, до яких вона застосовується, повинні бути тими, які стоять на стороні користувача.

Для створення криптокарти треба використати команду crypto map <name> <sequence-num> <type> в режимі глобальної конфігурації, щоб увійти в режим конфігурації криптокарти для цього порядкового номера. Кілька тверджень криптокарти можуть належати до однієї і тієї ж криптокарти і оцінюються у порядку зростання. Необхідно увійти у режим конфігурації криптокарти на R1, використовуючи тип ipsec-isakmp, який говорить про те, що IKE використовується для створення безпечного з'єднання IPsec.

1. Створити криптокарту на R1 з назвою CMAP та порядковим номером 10. Після введення команди з'являється повідомлення.

```
R1(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer and
a valid access list have been configured.
```

2. Скористатися командою match address <access-list>, щоб вказати список доступу, який визначає трафік для шифрування.

```
R1(config-crypto-map)# match address 101
```

3. Щоб переглянути список можливих заданих команд, які можна виконати з криптокартою, необхідно скористатися довідковою функцією.

```
R1(config-crypto-map)# set ?
  identity              Identity restriction.   ip
Interface Internet Protocol config commands   isakmp-profile
Specify isakmp Profile   nat                    Set NAT translation
peer                  Allowed Encryption/Decryption peer.
  pfs                   Specify pfs settings   reverse-
route         Reverse Route Injection.
  security-association  Security association parameters
  transform-set         Specify list of transform sets in priority order
```

4. Встановлення IP-адреси або імені користувача обов'язкове. Варто встановити його на віддалений інтерфейс кінцевої точки VPN R3 за допомогою наступної команди.

```
R1(config-crypto-map)# set peer 10.2.2.1
```

5. Використати команду set transform-set <tag>, щоб жорстко кодувати набір перетворень, який буде використовуватися з цим користувачем. Треба встановити тип секретності переадресації, використовуючи команду set pfs <type>, і змінити час життя безпечного зв’язку IPsec за замовчуванням за допомогою команди set security-association lifetime seconds <seconds>.

```
R1(config-crypto-map)# set pfs group14
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config-crypto-map)# exit
```

6. Створити відповідну криптокарту на R3.

```
R3(config)# crypto map CMAP 10 ipsec-isakmp R3(config-crypto-map)#
match address 101
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set pfs group14
R3(config-crypto-map)# set transform-set 50
R3(config-crypto-map)# set security-association lifetime seconds 900
R3(config-crypto-map)# exit
```

7. Застосувати криптокарту до інтерфейсів.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map CMAP
*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)# end

R3(config)# interface S0/0/1
R3(config-if)# crypto map CMAP
*Jan 28 04:10:54.138: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config)# end
```

Завдання 2: Перевірка конфігурації Site-to-Site VPN з тунелюванням IPsec.

1. Використання розширеного пінгу від R1 до IP-адреси інтерфейсу R3 F0/1 192.168.3.1 дозволяє контролювати адресу джерела пакетів.

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.3.1
Repeat count [5]: Datagram
size [100]: Timeout in seconds
[2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1 Type
of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]: Data
pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]: Type
escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.1 ..!!!
Success rate is 100 percent (3/5), round-trip min/avg/max = 92/92/92 ms
```

З виводу команди ми бачимо, що є зв’язок між двома віддаленими клієнтами.

2. Вводячи команду show crypto isakmp sa, бачимо, що створено безпечний зв’язок між маршрутизаторами R1 та R3.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA dst              src             state
conn-id status 10.2.2.1        10.1.1.1        QM_IDLE
1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

4.2 Налаштування Remote Access VPN з використанням технології тунелювання IPsec

На відміну від розглянутої у попередньому пункті реалізації Site-to-Site VPN, де тунелі створюються між маршрутизаторами віддалених мереж, дуже великим попитом користується метод VPN віддаленого доступу - Remote Access.

Remote Access VPN використовується для віддаленого доступу до корпоративного офісу з, наприклад, невеликого офісу або домашнього офісу (SOHO). При цьому, майже всі налаштування виконуються на виділеному маршрутизаторі головного офісу, який виступає у ролі VPN серверу. Для того, щоб користувач зміг отримати доступ до мережі головного офісу, достатньо лише наявності встановленого та попередньо налаштованого клієнтського програмного забезпечення на його ПК, на зразок Cisco VPN Client, Cisco AnyConnect та інші.

У цій частині диплома описано побудову багатокористувацької мережі та налаштування маршрутизаторів і хостів. Налаштовується VPN для віддаленого доступу між клієнтським комп'ютером та імітованою корпоративною мережею. Налаштування маршрутизаторів можливо виконати як за допомогою інтерфейсу командного рядку (CLI), так і більш наглядного та зрозумілого для користувача інструмента Cisco Security Device Manager (SDM). Cisco SDM – це програма з використанням веб-інтерфейсу, за допомогою якого можливо як налаштовувати всі пристрої з Cisco IOS, так і виконувати моніторинг основних процесів у реальному часі.

SDM використовується для налаштування сервера Cisco Easy VPN на корпоративному маршрутизаторі (граничному шлюзі за замовчуванням) та налаштування клієнта VPN Cisco на хості. Потім відбувається підключення до корпоративної мережі через модельований маршрутизатор провайдера.

VPN Клієнт Cisco дозволяє організаціям встановлювати наскрізні зашифровані IPsec VPN тунелі для безпечного підключення віддалених користувачів. Він підтримує Cisco Easy VPN, що дозволяє клієнту отримувати політику безпеки при підключенні до тунелю VPN від центрального пристрою VPN (Cisco Easy VPN Server), мінімізуючи вимоги до конфігурації у віддаленій мережі. Це масштабоване рішення для розгортань віддаленого доступу, де індивідуально налаштовувати політики для декількох віддалених ПК є недоцільним.

Топологія з’єднань та основних налаштувань експериментального стенду показана на рисунку 4.2.

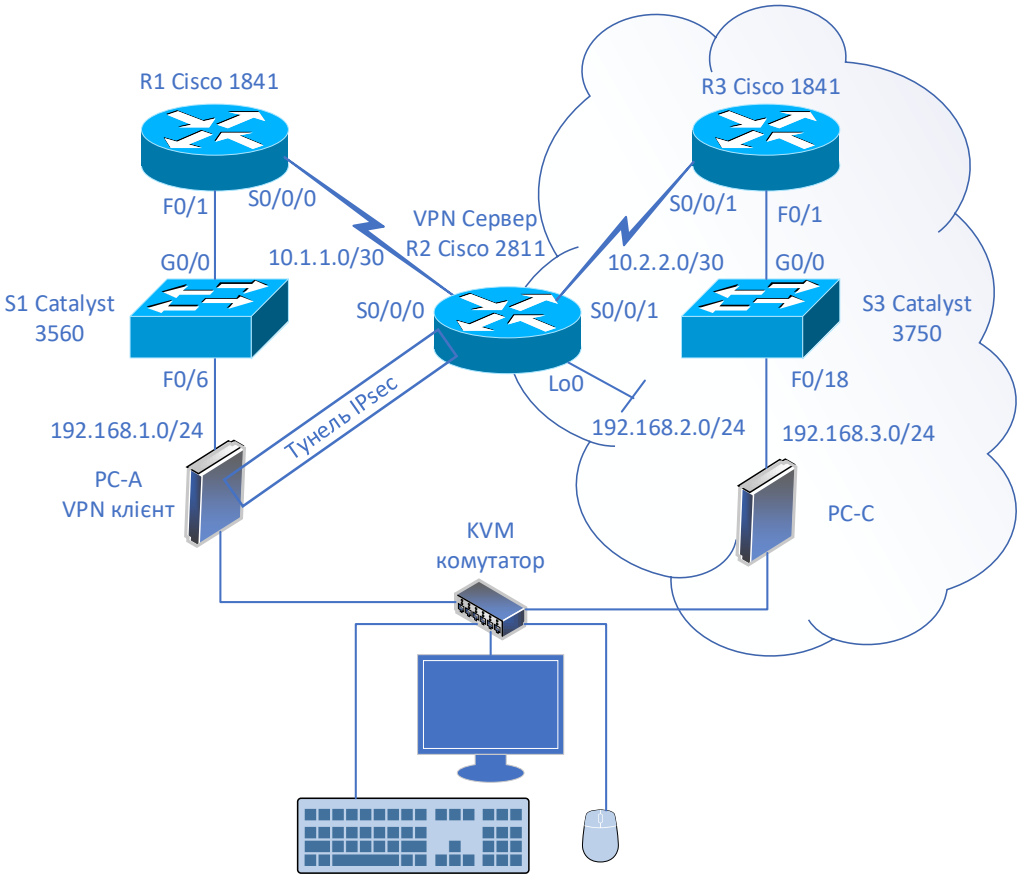

Рисунок 4.2 – Топологія мережі для сценарію Remote Access VPN

Перелік основного обладнання, модулів та кабелів залишається таким самим, як і в попередньому пункті даної роботи (табл. 4.2).

Таблиця 4.2 - IP-адресація

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Порт комутатора
R1	F0/1	192.168.1.1	255.255.255.0	N/A	S1 G0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Loopback 0	192.168.2.1	255.255.255.0	N/A	N/A
R3	F0/1	192.168.3.1	255.255.255.0	N/A	S3 G0/0
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Цілі:

Частина 1: Базова конфігурація маршрутизаторів

- Налаштування імен хостів, IP-адрес інтерфейсів та паролів доступу.
- Налаштування динамічного протоколу маршрутизації EIGRP на R2 та R3.

Частина 2: Налаштування VPN віддаленого доступу (Remote Access)

- Налаштування маршрутизатора для підтримки сервера Easy VPN за допомогою програми SDM.
- Налаштування клієнта VPN Cisco на ПК-А та підключення до R2.
- Перевірка конфігурації.
- Перевірка функціональності VPN.

Необхідні ресурси:

- 3 маршрутизатори зі встановленим SDM 2.5 (Cisco 1841 з Cisco IOS версії 15.1 (4) M12A з ліцензією технологічного пакета безпеки – advipservicesk9, Cisco 2811 з Cisco IOS версії 15.1 (4) M10 з ліцензією технологічного пакета безпеки - advipservicesk9)
- 2 комутатори (Cisco 3560-48TS-S та 3750-48PS-S)
- 2 ПК (Windows, програма Putty з терміналом та клієнтом SSH)
- Послідовний (Serial) і Ethernet-кабелі, як показано в топології
- WAN-модулі WIC-2T для зв’язку між маршрутизаторами
- Консольні кабелі для налаштування мережевих пристроїв Cisco

Частина 1: Базова конфігурація маршрутизаторів

Крок 1: Підключення мережі, як показано в топології (рис. 4.2).

Під’єднання пристроїв, що показані на топологічній схемі.

Крок 2. Налаштування основних параметрів для кожного маршрутизатора (табл. 4.2).

1. Налаштування імен хостів, як показано в топології.
2. Налаштування IP-адрес фізичних інтерфейсів, як показано в таблиці 4.2 IP-адресації.

3. Налаштування інтерфейсу логічної петлі Loopback0 на R2. Це імітує мережу, з якої клієнти віддаленого доступу отримують адреси (192.168.2.0/24).

```
R2(config)# interface Loopback 0
R2(config-if)# ip address 192.168.2.1 255.255.255.0
```

4. Налаштування тактової частоти для послідовних інтерфейсів маршрутизатора за допомогою приєднаного послідовного кабелю DCE

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

Крок 3: Вимкнути пошук DNS.

Необхідно відключити пошук DNS, щоб маршрутизатор не намагався інтерпретувати неправильно введені команди.

```
R1(config)# no ip domain-lookup
```

Крок 4: Налаштування протоколу маршрутизації EIGRP на R2 та R3.

R1 діє як маршрутизатор Інтернет сервіс-провайдера (ISP) і не бере участі в процесі маршрутизації EIGRP.

1. На R2 ввести наступні команди:

```
R2(config)# router eigrp 101
R2(config-router)# network 10.1.1.0 0.0.0.3
R2(config-router)# network 10.2.2.0 0.0.0.3
R2(config-router)# network 192.168.2.0 0.0.0.255
R2(config-router)# no auto-summary
```

2. На R3 ввести наступні команди:

```
R3(config)# router eigrp 101
R3(config-router)# network 192.168.3.0 0.0.0.255
R3(config-router)# network 10.2.2.0 0.0.0.3
R3(config-router)# no auto-summary
```

Крок 5: Налаштування статичного маршруту за замовчуванням до R2.

Маршрутизатор R1 надає з'єднання з інтернетом. Маршрут за замовчуванням налаштований на R2 для всього трафіку, мережі призначення якого не існує в таблиці маршрутизації R2.

1. Налаштування статичного маршруту за замовчуванням на R2, який вказує на IP-адресу інтерфейсу R1 S0/0/0:

```
R2(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

2. Перерозподілення статичного маршруту за замовчуванням в EIGRP, щоб R3 також вивчив маршрут.

```
R2(config)# router eigrp 101
R2(config-router)# redistribute static
```

Крок 6: Налаштування параметрів IP хоста ПК.

1. Налаштувати статичну IP-адресу, маску підмережі та шлюз за замовчуванням для PC-A, як показано в таблиці 4.2 IP-адресації.
2. Налаштувати статичну IP-адресу, маску підмережі та шлюз за замовчуванням для PC-C, як показано в таблиці 4.2 IP-адресації.

Крок 7: Перевірка базового підключення до мережі.

Проведення пінг-запиту з PC-A на інтерфейс R2 S0/0/0 за IP-адресою 10.1.1.2 та від R2 до PC-C в локальній мережі R3.

Крок 8: Налаштування мінімальної довжини пароля.

Використати команду "security passwords", щоб встановити мінімальну довжину пароля в 10 символів.

```
R1(config)# security passwords min-length 10
```

Крок 9: Налаштування основних ліній консолі та ліній підключення vty за протоколом telnet.

1. Налаштувати пароль консолі та створити логін для маршрутизатора R1. Для додаткової безпеки команда exectimeout призводить до виходу з рядка після 5 хвилин бездіяльності. Команда logging-synchronous не дозволяє консольним повідомленням переривати введення команди.

```
R1(config)# line console 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

2. Налаштування пароля у рядках vty для маршрутизатора R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

3. Такий самий алгоритм для маршрутизаторів R2 та R3.

Крок 10: Шифрування відкритих текстових паролів.

1. Необхідно використати команду service password-encryption для шифрування паролів консолі, aux та vty.

```
R1(config)# service password-encryption
```

2. Такий самий алгоритм для маршрутизаторів R2 та R3.

Крок 11: Збереження основної робочої конфігурації для всіх трьох маршрутизаторів.

```
R1# copy running-config startup-config
```

Частина 2: Налаштування VPN віддаленого доступу

У частині 2 створюється IPsec VPN віддаленого доступу. R2 налаштований як сервер Easy VPN за допомогою SDM, а клієнт Cisco VPN налаштований на PC-A. Хост PC-A імітує співробітника, який намагається отримати доступ з дому через Інтернет. Маршрутизатор R1 імітує маршрутизатор Інтернет-провайдера.

Крок 1. Налаштування доступу за допомогою команди enable secret та маршрутизатора HTTP перед запуском SDM.

1. У командному рядку налаштувати секретний пароль командою enable secret для використання з SDM на R2.

```
R2(config)# enable secret cisco12345
```

2. Включити HTTP-сервер на R2.

```
R2(config)# ip http server
```

3. Створити акаунт admin з рівнем привілегії 15.

```
R2(config)# username admin privilege 15 password 0
cisco12345
```

Завдання 2: Використання програми SDM для налаштування Easy VPN сервера

Крок 1. Налаштування віртуального тунельного інтерфейсу та аутентифікації.

Обираємо pre-shared keys (відкритий ключ) як тип аутентифікації (рис. 4.3).

Рисунок 4.3 – Налаштування інтерфейсів та аутентифікації

Крок 2. У вікні пропозицій Інтернет-обміну ключами (IKE) пропозиція IKE за замовчуванням використовується для R2.

Крок 3. Обираємо набір перетворень ESP_3DES.

Крок 4. Налаштування аутентифікації користувача (рис. 4.4)

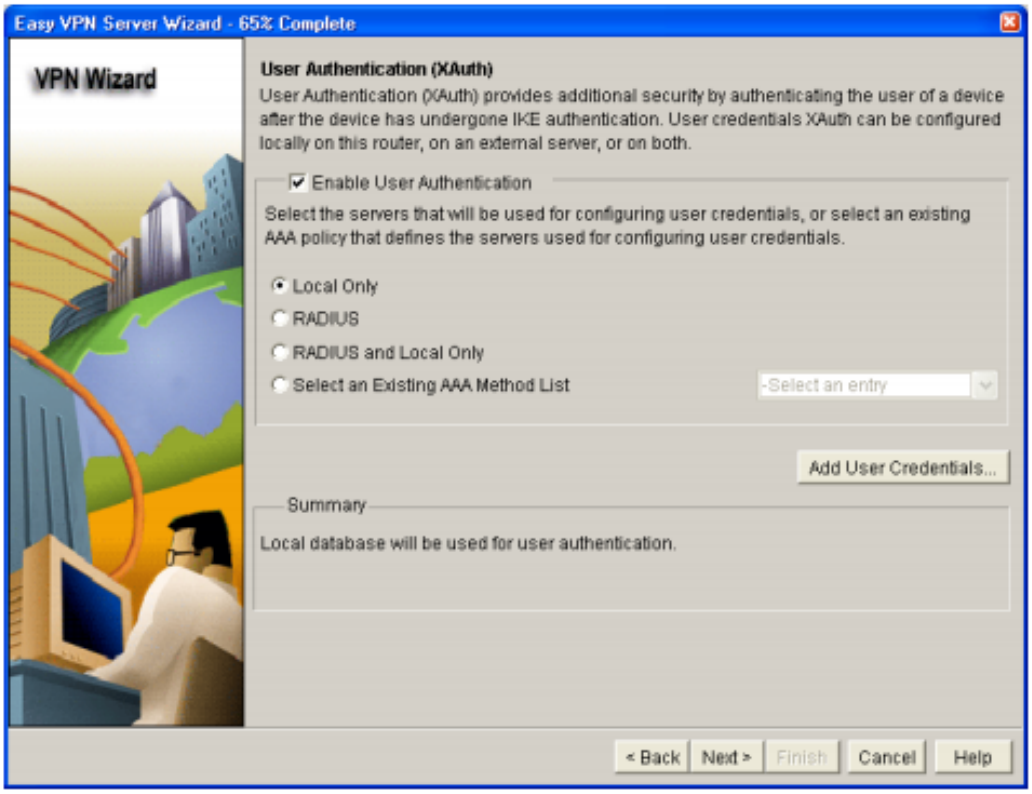

Рисунок 4.4 –Аутентифікація користувача

Крок 5. Додання облікових даних для іншого користувача (рис. 4.5)

Логін – admin01, пароль - user01pass. Також оберемо алгоритм хешування MD5 та рівень привілейованості 1.

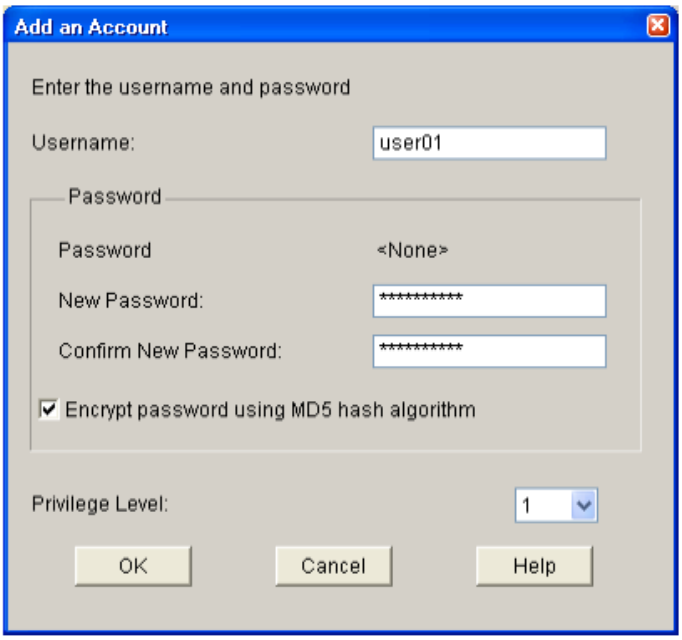

Рисунок 4.5 – Створення акаунту

Таким чином, з’явився новий акаунт (рис. 4.6)

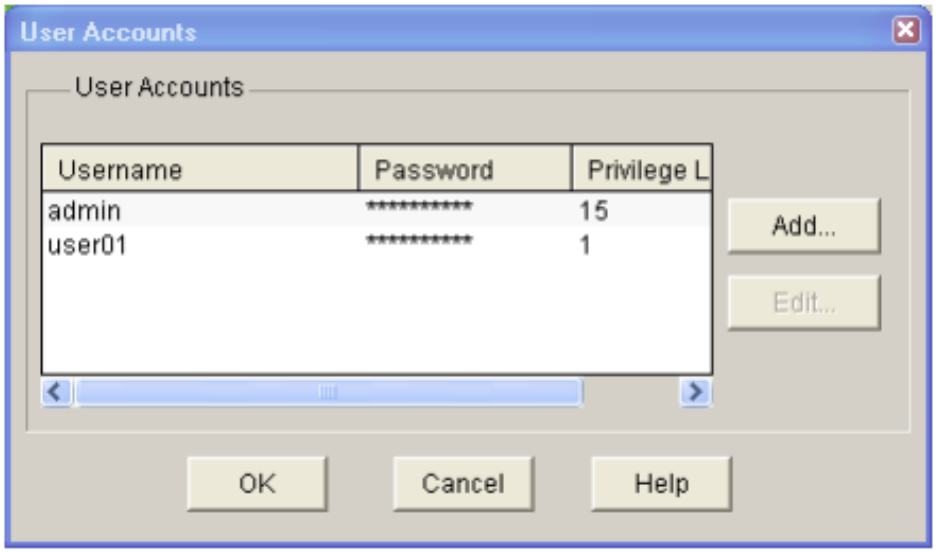

Рисунок 4.6 – Перевірка акаунтів

Крок 6. Додання політик групової авторизації користувачів.

Ім’я групи – VPN-Access, відкритий ключ – cisco12345, також обираємо максимальну кількість – 50.

Крок 7: Після завершення конфігурації обрати «deliver»

Завдання 3: Використання Cisco VPN Client для перевірки VPN віддаленого доступу.

Обрано до використання ПЗ Cisco VPN Client, оскільки воно має мінімальні системні вимоги до клієнтського обладнання, що дає можливість використання наявних у експериментальному стенді системних міні-блоків.

В даний час існує велика кількість програм, що виконують роль VPN-клієнта, в тому числі й компанія Cisco Systems продовжує розвивати цей програмний продукт.

Крок 1: Вводимо дані групової авторизації користувачів (рис. 4.7)

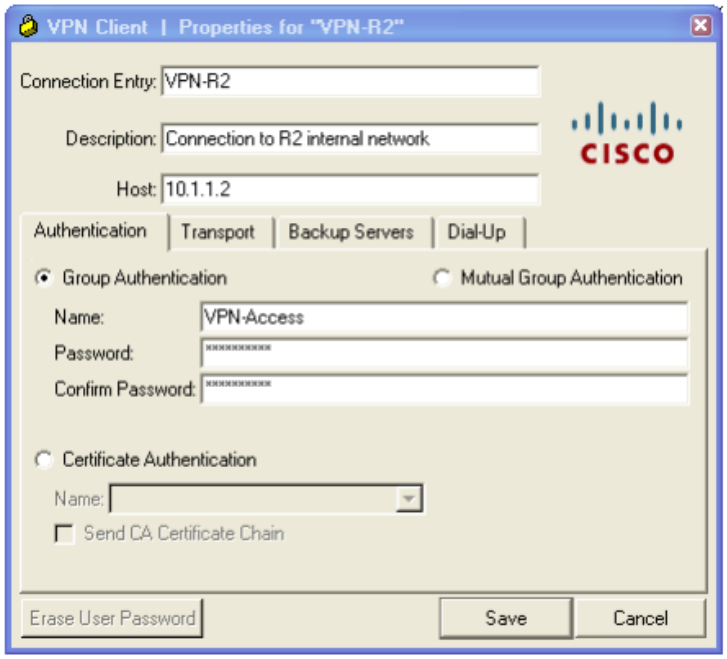

Рисунок 4.7 – Властивості групової авторизації користувачів

Крок 2: Виконання з'єднання

Вводячи дані авторизації та натиснувши Connect, відбувається з'єднання (рис. 4.8).

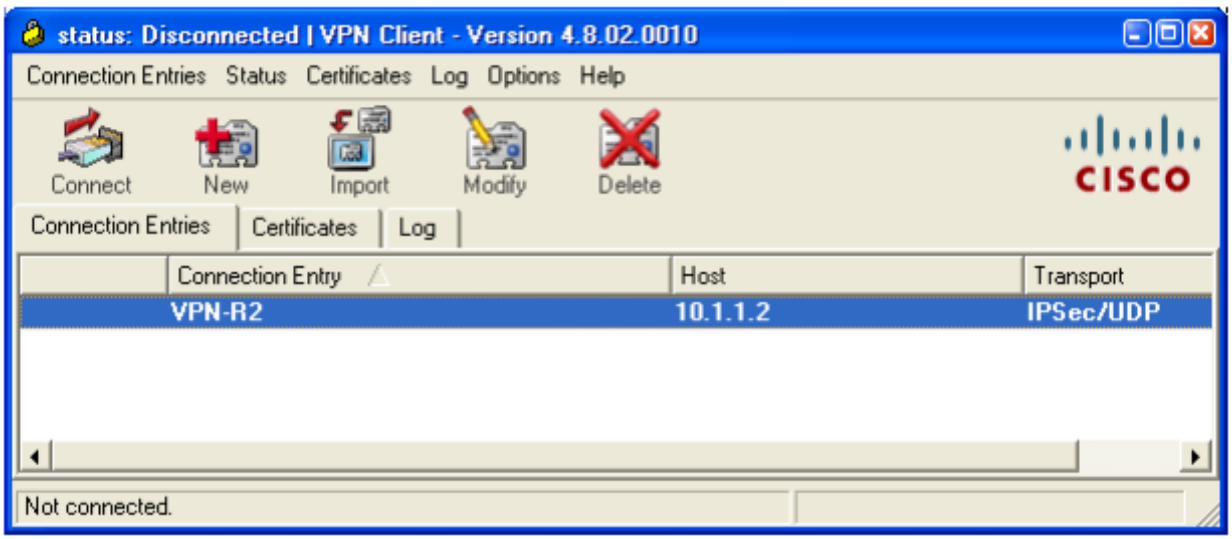

Рисунок 4.8 – Статус з'єднання

Завдання 4: Перевірка тунелю між клієнтом та сервером

Крок 1: Перевірка відповідних даних у вкладці Tunnel Details (рис. 4.9).

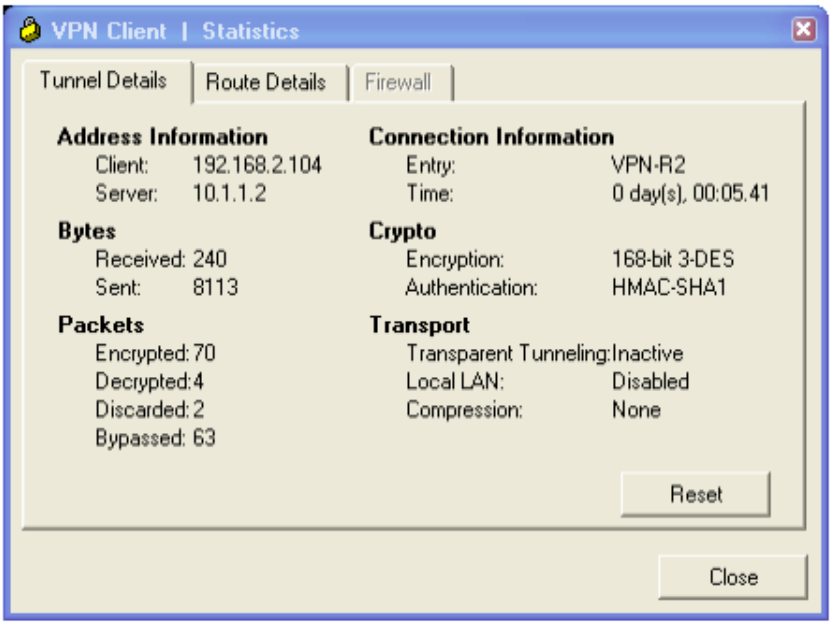

Рисунок 4.9 – Параметри тунелю

Крок 2: Перевірка VPN зв'язку.

Після введення команди ipconfig /all на PC-A маємо:

```
C:\ ipconfig /all

Windows IP Configuration
Host Name . . . . . . . . . . . . : PC-A
Primary Dns Suffix . . . . . . . :
Node Type . . . . . . . . . . . . : Hybrid
IP Routing Enabled. . . . . . . . : No
WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . . . . . . . . : VIA Networking
Velocity-Family Gigabit Ethernet Adapter
Physical Address. . . . . . . . . : 00-60-72-24-BF-29
Dhcp Enabled. . . . . . . . . . . : No
IP Address. . . . . . . . . . . . : 192.168.1.3
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . :
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
Description . . . . . . . . . . . : Cisco Systems VPN
Adapter
Physical Address. . . . . . . . . : 00-05-9A-3C-78-00
Dhcp Enabled. . . . . . . . . . . : No
IP Address. . . . . . . . . . . . : 192.168.2.104
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.2.1
```

Видно, що у комп’ютера PC-A з початковою адресою 192.168.1.3, завдяки побудованому IPsec тунелю, з’явилась друга IP-адреса 192.168.2.104, яка належить віддаленій мережі. Через це вдалося досягти ip-адреси PC-C, яка знаходиться у віддаленій мережі, що під’єднана до VPN-сервера (R2), оскільки PC-C знаходиться у тій самій групі доступу VPN, що й адреса 192.168.2.104.

4.3 Висновки до розділу 4

Даний розділ присвячено налаштуванню:

- технології Site-to-Site VPN з використанням технології тунелювання IPSec;
- технології Remote Access VPN з використанням технології тунелювання IPSec;

Всі налаштування виконувались на експериментальному стенді, описаному у попередньому розділі. В процесі роботи над розділом були здобуті наступні навички:

- Налаштування маршрутизаторів для створення захищених тунелів при реалізації технології Site-to-Site VPN;
- Налаштування VPN серверу та клієнтських маршрутизаторів для створення захищених тунелів при реалізації технології Remote Access VPN;
- Освоєння програмного забезпечення Cisco Security Device Manager (SDM) для налаштування та моніторингу маршрутизаторів;
- Освоєння програмного забезпечення Cisco VPN Client для створення захищеного тунелю між клієнтом та VPN сервером.

Особливо слід зазначити, що технологія IPsec VPN, якій приділено велику увагу у даному розділі, є основою для більш поглиблених варіантів створення захищених тунелів, таких як VTI VPN, DMVPN та Flex VPN.

ВИСНОВКИ

У сучасному світі, де різні інформаційні технології тісно інтегровані не тільки у великі корпоративні мережі, а й у побут звичайних користувачів, реалізація віртуальних приватних мереж з обов'язковим використанням протоколів безпеки стає критично необхідною. Захисту мають підлягати буквально усі сфери людської діяльності, починаючи з персональних даних звичайних користувачів і закінчуючи мережами великих корпорацій та сервіс-провайдерів. Все частіше збитки від різноманітних кіберзагроз навіть важко оцінити.

Таким чином, в даній роботі проаналізовано засоби забезпечення безпеки мережевого трафіку, пояснені призначення та особливості технології віртуальних приватних мереж (VPN), необхідність тунелювання, шифрування, аутентифікації та забезпечення цілісності даних.

З'ясовано, що технологія VPN призначена для захисту мережевої взаємодії між географічно розподіленими користувачами, може бути реалізована на різних рівнях моделі OSI та виконана у різних реалізаціях, в залежності від необхідного функціоналу, розміру мереж та передбаченого навантаження на них.

Зазначено, що VPN використовують тунелювання за допомогою протоколів IPsec, L2TP, PPTP та SSL, шифрування трафіку для забезпечення конфіденційності даних, аутентифікацію користувача та алгоритми забезпечення цілісності даних.

Наведено класифікацію віртуальних приватних мереж на основі брандмауера, на основі апаратних засобів, на основі програмного забезпечення та SSL VPN і розглянуті їх особливості.

Досліджено мережі VPN рівня 2 і 3 та надана їх порівняльна характеристика. Основними відмінностями VPN рівня 3 є визначення політик та маршрутизації постачальником послуг і необхідність клієнтів ділитися інформацією про топологію своєї мережі. Також комутатор клієнта повинен

бути налаштований на використання BGP або OSPF для зв'язку з комутатором постачальника послуг.

Проаналізовані особливості функціонування технології MPLS VPN та зазначено, що перевагами цієї технології є сервіс без встановлення з’єднання, непотрібність тунелів для шифрування та конфіденційності мережі, централізоване обслуговування, масштабованість, підтримка якості обслуговування (QoS).

Були досліджені основні технології тунелювання, визначені принципи їх роботи, призначення та сфери застосування у віртуальних приватних мережах. Було проаналізовано основні реалізації VPN: Remote Access – для зв’язку між географічно розподіленими філіями та Site-to-Site – для доступу користувачів до ресурсів корпоративної мережі з віддалених робочих місць.

Особливу увагу приділено протоколу IPsec як базі для функціонування захищених з’єднань, його принцип обміну ключами, аутентифікацію та режими роботи.

Провідним виробником активного обладнання для мережі Інтернет вже кілька десятиліть залишається корпорація Cisco Systems, яка не тільки є виробником обладнання, але й розробником міжнародних стандартів в області телекомунікацій. Тому особливу увагу в цій роботі було приділено реалізації віртуальних приватних мереж саме на рішеннях від Cisco.

Робота також має велику практичну цінність, оскільки значну її частину становить технічна реалізація віртуальних приватних мереж на основі власноруч побудованого та налаштованого експериментального стенду. Опанування синтаксису командного рядку операційної системи Cisco IOS дозволило налаштувати та перевірити роботу Site-to-Site та Remote Access VPN – двох базових реалізацій даної технології.

Безпеку передачі даних може бути досягнуто різними методами, в залежності критичності даних та технічних можливостей самих мереж. Найкращим є рішення, що водночас забезпечує тунелювання, шифрування, аутентифікацію та цілісність даних. Основою створення захищених VPN є

застосування протоколу безпеки IPsec у побудованих тунелях, оскільки його принцип створення та обміну ключами, аутентифікації вже довгий час є стандартом для мереж з критичним трафіком та дозволяє розробляти більш поглиблені варіанти створення захищених тунелів, такі як VTI VPN, DMVPN та Flex VPN.

ПЕРЕЛІК ПОСИЛАНЬ

1. Доповідь «Побудова віртуальних приватних мереж на основі обладнання фірми Cisco», Конференція «Проблеми Телекомунікацій», 2020. – 3 с. – Волік Д.В., Григоренко О. В.
2. [Електронний ресурс] – Режим доступу: https://www.comparitech.com/vpn/vpn-statistics/
3. VPN Security - The Government of the Hong Kong Special Administrative Region, 2008 – 24 с.
4. [Електронний ресурс] – Режим доступу: https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-ex-series-vpn-layer2-layer3.html
5. MPLS Layer 3 VPNs Configuration Guide, Cisco, 2011. – 310 с.
6. [Електронний ресурс] – Режим доступу: http://ciscotips.ru/vpn
7. IPSec VPN Configuration, Cisco, 2009. – 28 с.
8. The Complete Cisco VPN Configuration Guide By Richard Deal, 2005. – 1032с.
9. Point-to-Point GRE over IPsec Design Guide. – Cisco, 2006. – 106 с.
10. Cisco IOS VPN Configuration Guide, 2005. – 131 с.